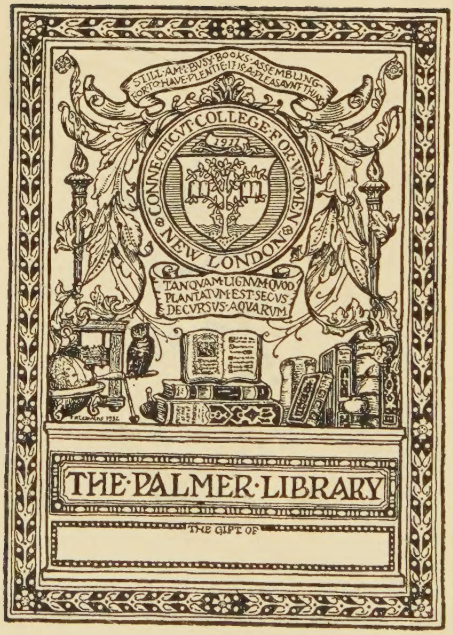

STILL AM I BUSY BOOKS ASSEMBLING
FOR TO HAVE PLENTIE IT IS A PLEASOVNT THING
CONNECTICVT COLLEGE FOR WOMEN
NEW LONDON
TAN QVAM LIGNVM QVOD
PLANTATVM EST SECVS
DECVRSVS AQVARVM
THE PALMER LIBRARY
THE GIFT OF

ELEMENTARY THEORY OF FINITE GROUPS

BY

LOUIS CLARK MATHEWSON

Professor of Mathematics in Dartmouth College

UNDER THE EDITORSHIP OF

JOHN WESLEY YOUNG

Late Professor of Mathematics, Dartmouth College

HOUGHTON MIFFLIN COMPANY

BOSTON · NEW YORK · CHICAGO · DALLAS

ATLANTA · SAN FRANCISCO

The Riverside Press Cambridge

512 86
M426

COPYRIGHT, 1930
BY LOUIS CLARK MATHEWSON

ALL RIGHTS RESERVED INCLUDING THE RIGHT TO REPRODUCE
THIS BOOK OR PARTS THEREOF IN ANY FORM

The Riverside Press
CAMBRIDGE · MASSACHUSETTS
PRINTED IN THE U.S.A.

EDITOR'S INTRODUCTION

THE idea of a group is one of those truly fundamental concepts of mathematics with which every serious student of the subject must sooner or later make himself familiar. Although implicit in almost every part of mathematics from the earliest times to the present, it was not specifically formulated until relatively recent times. This perhaps accounts for the fact that hitherto there has been no elementary textbook on this subject in English. Professor Mathewson's little book will, therefore, fill a very definite need in the more advanced mathematical instruction in English-speaking countries.

It will doubtless find considerable use as a text for courses in this subject. Many students, however, find it difficult to include such a course in their work and yet are expected to be familiar with the fundamental ideas and theorems of this subject. It will, therefore, be found distinctly useful also for self study on the part of such students.

I am very glad indeed to see it appear as one of the series of texts which I am editing.

JOHN W. YOUNG

93397

Digitized by the Internet Archive
in 2023 with funding from
Kahle/Austin Foundation

https://archive.org/details/elementarytheory0000loui

PREFACE

THIS is an elementary textbook in the theory of finite groups. It is, accordingly, suited to graduate or advanced undergraduate students beginning a study of this subject. A background of some topics in higher or modern algebra, theory of equations, and theory of algebraic numbers would be desirable. However, mathematical insight and some degree of mathematical maturity are sufficient prerequisite.

The text aims to be both teachable and understandable. To this end the presentation is not in monograph or dissertation style, but is largely by proposition and proof, a method which offers the student definite, assimilable units. Again, there is considerable coherence in the organization of the material of the book effected partly by many cross-references, principally back references, which serve to coördinate and reënforce the subject-matter in the student's mind. Most of the chapters have been tried out once or more in the classroom. A few theorems are here put into print for the first time, it is believed, and the proofs of some older ones have been simplified.

In teaching from the text too much emphasis cannot be laid on the use of the numerous exercises throughout. Some are simpler and merely make the reader familiar with definitions and theorems; some require more constructive work; many are a part of the theory and as such are referred to in the course of the book. The beginner, therefore, will benefit by solving practically all of them.

The some fifty "additional exercises" listed at the ends of the chapters are to enlarge the student's contacts and to furnish supplementary material where it can be used, as with the better

student. Referring to other texts will acquaint him with other methods, other applications, other fields. Besides the attempt to select suitable exercises, the author has for convenience in assignments made the references to material for these exercises diversified in each set. These "additional exercises" are not necessary to the understanding of the rest of the text, hence they help in making it adaptable to different classes and offer variety for supplementary topics and flexibility in length of course.

Bibliographies of the literature on various topics in group theory are out of place in this book.* Chapter X on the Lagrange-Galois theory of algebraic equations and the Lie one-parameter groups in differential equations, is purposely sketchy. For a study of either of these topics the reader might well use textbooks to which reference is made.†

The author's thanks are due those who have made this little book possible, especially to Professor J. W. Young for constructive suggestions.

LOUIS C. MATHEWSON

HANOVER, N.H.

* For such lists the following may be consulted:
Easton, *Constructive Development of Group Theory* (University of Pennsylvania, 1902).
Miller, "Reports in Group Theory," in *The Bulletin of the American Mathematical Society*, vol. v (1899), p. 227; vol. VII (1900), p. 121; vol. IX (1902), p. 106; vol. XIV (1907), pp. 78, 124.
Alasia, "Essai d'une bibliographie sur la théorie des groupes," in *Revista di fisica, mathematica e scienze naturali* (Pavia, 1908–10).
Chatelet, *Les Groupes Abeliens Finis et les Modules de Points Entières* (Gauthier-Villars, 1925), pp. 223–33.

† For some interesting group theory questions awaiting solution see:
Hilton, H., *Finite Groups* (Clarendon Press, 1908), p. 233.
Carmichael, R. D., in *The American Mathematical Monthly*, vol. 36 (1929), pp. 142, 143.

CONTENTS

CHAPTER I

Examples of Groups and Some Definitions

1. Example One 1
2. Example Two 3
3. Example Three 5
4. Notation and General Definition of a Group . . 5

CHAPTER II

Permutations and Permutation Groups

5. Illustration 8
6. Notation and Definitions 9
7. Product of Permutations 12
8. Symmetric Group on Three Letters 15
9. Symmetric Group on n Letters 16
10. Theorems on Permutations 18
11. Some General Theory of Finite Groups 22
12. Some Theorems on Permutation Groups 27

CHAPTER III

Permutation Groups, Continued: Transitivity and Primitivity

13. Illustration and Definitions 33
14. Elementary Theorems on Transitive Groups . . . 33
15. Conjugate Set of Elements 36
16. Conjugate Set of Subgroups 39
17. Theorems Involving Conjugates 40
18. Multiple Transitivity 43
19. Primitive and Imprimitive Groups 45

20. Isomorphisms 49
21. Construction of Intransitive Groups 52
22. Invariant Subgroups of Symmetric and Alternating Groups 55
23. Groups of Degrees Two, Three, and Four 58

CHAPTER IV

Some Groups of Movements and Other Special Groups

24. Introduction 62
25. Group of the Square 63
26. Group of the Regular Tetrahedron 64
27. A Group of Line Movements and a Group of Paths . 65
28. Group of Certain Operations on a Given Angle . . 68
29. Group Generated by an Imaginary nth Root of Unity 69
30. Certain Congruence Groups 69
31. Quaternion Units and Matrices as Elements . . . 71

CHAPTER V

Some General Properties of Groups

32. Review 74
33. Transforms and an Application 74
34. More About Conjugates 75
35. Commutators 77
36. On the Quotient Group 80
37. On Prime-Power Subgroups 82
38. Sylow's Theorem 83

CHAPTER VI

On Abelian Groups

39. On the Cyclic Group 87
Notes from Number Theory 88
40. Subgroups of an Abelian Group 89
41. Prime-Power Abelian Groups 91
42. On the Abelian Group of Order p^m, Type (1, 1, etc.) . 93

CHAPTER VII

On Abstract Definitions and Some Well-Known Groups

43. Introduction 95
44. Abstract Definitions of Some Well-Known Groups . 96
45. On Prime-Power Groups 98
46. An Application 101
47. Hamiltonian Groups 104

CHAPTER VIII

The Group of Isomorphisms and the Composition-Series

The Group of Isomorphisms

48. Examples and Definitions 107
49. Inner and Outer Isomorphisms 110
50. On Automorphisms of Abelian Groups 110
51. Additional Theory 114
52. Two Applications 116

Composition-Series

53. Definitions and Examples 118
54. The Jordan-Hölder Theorems 119
55. Solvable and Insolvable Groups 121
56. Other Series of Included Groups 122

CHAPTER IX

On Groups of Linear Substitutions

57. Introduction 125
58. The Linear Substitution Group 127
59. Hermitians 129
60. Absolute and Relative Invariants 132
61. Characteristic Equation of a Linear Substitution . 133
62. Lemmas on Invariants 134
63. Reducible and Irreducible Linear Substitution Groups 136

CHAPTER X

Some Applications of Group Theory in Other Fields

64. Topics in This Chapter 141

An Outline of the Lagrange-Galois Theory

65. Preliminary Ideas 141
66. Preliminary Theory 142
67. Lagrange's and Galois' Theories 145
68. Group of the General Equation 146
69. Further Galois Theory 147
70. Criterion of Solvability 149
71. Examples of Adjunction 151

Constructions by Ruler and Compasses

72. On Constructibility. Duplication of the Cube; Trisection of an Angle 154

A Note on Lie's Theory

73. A One-Parameter Transformation Group 156
74. Some Theorems 157
75. An Application 159

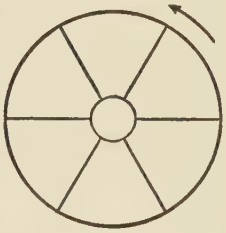
Index 163

ELEMENTARY THEORY OF FINITE GROUPS

CHAPTER I

EXAMPLES OF GROUPS AND SOME DEFINITIONS

1. Example One. All our thinking is said to be concerned with percepts and concepts, with the drawing of conclusions on comparing these, and with deducing new conclusions from old ones. Accordingly, in these notes examples are frequently used to introduce new ideas or theory. To develop the concept of a group let us study certain rotations of a six-spoke wheel as it turns about its axis. Suppose the rotations are counter-clockwise and each such that it leaves the wheel with one pair of spokes horizontal. Since consecutive spokes are 60° apart, rotations must be multiples of 60°. Suppose A represents a rotation of the wheel from any of its positions counter-clockwise through 60°, B through 120°, C through 180°, D through 240°, E through 300°, and finally I through 360° a rotation which brings every spoke back into its original position.



Evidently if any two of these six rotations are performed in succession, the result is equivalent to some rotation in the set. Thus, rotation through 120° followed by rotation through 300°

brings the wheel to the same position as would rotation through 60°. In general, if the elements of a set are such that combining any one with any one gives an element of the set, it is known as a **closed set.** There are four properties which a set must possess in order that it be a group, and that it be a closed set is probably the fundamental one. It is sometimes called "the group property."

The letters introduced may now be employed to test combinations of rotations. To this end let AD mean the result of performing the rotation represented by A, followed by the rotation represented by D. Just as in some other theories similar expressions may not mean multiplication in the ordinary sense, so here they do not. However, "multiplication" is not infrequently employed in a general way, and here AD may be read "A multiplied by D," or "multiply A by D." It is easy to see that, with the above meanings,

$$AB = C, \quad AC = D, \quad AD = E, \quad AE = I, \quad AI = A,$$
$$BA = C, \quad BC = E, \quad BD = I, \quad BE = A, \quad BI = B, \text{ etc.}$$

Further, since AA would mean rotation through 60° followed by another rotation through 60°, $AA = B$. The convenience of exponents naturally suggests writing A^2 for AA. Similarly, $BB = B^2 = D$, $C^2 = I$, $D^2 = B$, etc., $A^3 = C$, $A^4 = D$, etc.

Before going on to discuss the three other group requirements, it should be noted that had any one of the rotations in this example been lacking, the set would not have been closed.

The second requirement is that the associative law hold in combining the members of the set. Thus, for B, D, A, $B(DA)$ must equal $(BD)A$; that is, B followed by (DA) is the same as (BD) followed by A.

Another requirement is the existence of a member which

when combined with any member of the set leaves this member individually unchanged, or as it was. Evidently, here it is the rotation through 360°, for $AI = IA = A$, $BI = IB = B$, etc. This member is called the **identity** and will be represented by I. In this example it might just as well have represented rotation through 0°.

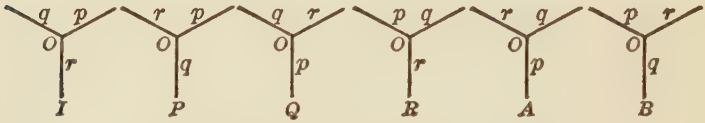
The fourth requirement is that for each member of the set there exist a member which combined with it will give the identity. Here, $AE = BD = CC = I$. Each of such a pair is known as the **inverse** of the other.

The members of a group are called **elements** (or **operators**) and the number of elements composing the group is its **order.** The set of rotations just considered satisfies the four requirements and is therefore a group. It is of order six.

In summarizing the requirements just pointed out, it may be said that a set of distinct elements with a law of combination is a group if (1) the set is closed with respect to the law of combination, (2) the associative law holds, (3) a single identical element is included, and (4) each element has an inverse in the set. Although these properties are necessary in order that a set be a group, they are not the only properties a group may have. While in Example One any two elements were commutative; that is, $AB = BA$, $AC = CA$, $BD = DB$, etc., there are many groups containing some pairs of **non-commutative** elements. Example Two will bring out points of dissimilarity with the preceding group.

2. Example Two. Consider next another group of movements. Let three half lines, p, q, r, of a plane radiate from a point O such that each makes an angle of 120° with each of the others, and let a line l pass through O perpendicular to the plane

of the three lines. The movements are to be rotations about l, p, q, r which bring the plane into itself and which are such that p always has one of the three original positions of p, q, r. Suppose P, Q, R represent rotations of 180° (in either direction) about p, q, r, respectively; and that A represents rotation about l such that p is replaced by q, q by r, and r by p; and B rotation about l such that p is replaced by r, r by q, and q by p; and that I represents the null or identical rotation. Let the set I, A, B, P, Q, R be tested for the group requirements. The positions are represented in the following figures.



There is an identity (I). In regard to inverses, it is obvious that since $P^2 = I$, P has an inverse (itself); and similarly R and Q are their own inverses; and since $AB = BA = I$, A and B are inverses of each other. The associative law holds. It then remains to determine whether the set is closed. Evidently it is unnecessary to consider combinations with I. Multiplying A by the various elements gives: AA or $A^2 = B$, which is seen by performing rotation A twice; $AB = I$; $AP = Q$, which is seen by performing upon A rotation through 180° about p; similarly, $AQ = R$; and $AR = P$. If B is followed by each rotation of the set, only elements of the set are obtained; and so on for all products, showing that the set is closed. Thus the set constitutes a group of order six.

But this group differs from the one in Example One, although they are of the same order. In the first group any two elements were commutative; *e.g.*, $DE = ED$. But here, notice

that while $AB = BA$, $AP \neq PA$, for $AP = Q$ while $PA = R$. Similarly, $PQ = B$ but $QP = A$. Hence A and B are commutative, but A and P are not; neither are P and Q. Thus the two groups differ considerably, for in the first all pairs of elements are commutative, but in the second some pairs are non-commutative. Commutativity is an important property in group theory and will be considered further in later chapters.

3. Example Three. Take the set of four numbers: $+1, -1, +i, -i$, where $i = +\sqrt{-1}$. In the first two examples the elements were rotations and the process of combining them consisted in following one rotation by another. Here, let the elements be the four numbers and let the process for combining them be ordinary multiplication.

It is not difficult to show that the set forms a group. In the first place, evidently the set is closed; for

$$i \cdot 1 = i, \qquad -1 \cdot i = -i,$$
$$i \cdot i = -1, \qquad -i \cdot i = 1, \text{ etc.}$$

The associative law holds in the multiplication of numbers, hence it holds for this set. There is one and only one element satisfying the requirements for the identical element; viz., $(+1)$. Lastly, there is an inverse for each element; for

$$(+1) \cdot (+1) = (+1),$$
$$(-1) \cdot (-1) = (+1), \qquad (+i) \cdot (-i) = (+1).$$

Hence, the set forms a group, which is of order four. Furthermore, since the multiplication of these numbers is commutative, this group like the one in Example One is a commutative group.

4. Notation, and General Definition of a Group. Symbols will now be employed to state the conditions necessary and

sufficient that a set of elements, each distinct from the others, forms a group.

Let A, B, C, etc., denote the operations or numbers or elements of the given set, and suppose a law of combination designated so that element A followed by element B (which may be any element of the set including A itself) determines some element, say C, uniquely. Symbolically this combining will be denoted by $AB = C$. The conditions then are:

(1) The set must be closed; *i.e.*, if A is any element of the set and B any element of the set, then the product AB must also be an element of the set.

(2) The associative law must hold; *i.e.*, if A, B, C are any elements of the set, $A(BC) = (AB)C$.

(3) There is one and only one identity, I; *i.e.*, an element such that $AI = IA = A$, where A is any element of the set.

(4) For each element, A, a single element (which may be represented by A^{-1}) exists such that $AA^{-1} = I$.

Notes. In AB, B is said to be multiplied on the left by A, and A on the right by B.

As was pointed out in the beginning of the chapter, if A is followed by itself the product AA is represented by A^2; similarly $AAA = A^2A = A^3$, etc.

If I is used to represent the identical element, evidently $A^0 = I$, and naturally then by the laws of exponents the inverse of A is A^{-1}, of A^2 is A^{-2}, etc.

Definitions. An element A is said to be of **period** n if n is the smallest positive integer for which $A^n = I$.

If various powers of some element of a group constitute all the elements, the group is said to be a **cyclic group.**

EXERCISES AND QUESTIONS

1. Determine whether either of the groups in Examples One and Two is cyclic.

2. Find an element in the group of Example Three, which when raised to successive powers gives all the elements of the group.

3. Discuss the group of an eight-spoke wheel for counter-clockwise rotation around its axis, if each rotation leaves the wheel with one pair of spokes horizontal.

4. If A, X, Y are elements of a group such that $AX = Y$, and if A remains fixed while X is in turn each of the elements of the group, show that the successive values of Y also are the elements of the group (in some order).

5. Determine the period of each element of the groups in Examples One and Two.

6. Show that an element of period 2 is its own inverse.

7. Show that $I = I^3 = I^5$, etc. Hint. Place $A = I$ in requirement (3).

8. If in requirement (3) I were defined such that for any element, B, of the group, $BI = B$, show that $IB = B$. Hint. Multiply each member of the equation on its left by BB^{-1} and simplify by requirements (2) and (4).

9. In requirement (4) prove that if $AA^{-1} = I$, then $A^{-1}A = I$. Hint. Let $A^{-1}X = I$, then show that $X = A$.

10. If the elements of a set satisfy the first three requirements and are distinct and finite in number, show that the requirement (4) is satisfied.

11. Show that $(AB)^{-1} = B^{-1}A^{-1}$.

12. If A and B are elements of a group, simplify the following (by removing parentheses): $(A^{-1}B^2)^{-1}$.

ADDITIONAL EXERCISES

1. Distinguish between finite and infinite groups. Give an illustration of a continuous group and of a discontinuous group. *Cf.* Burnside, *Theory of Groups* (1897 or 1911), § 14.

2. For definition of a *semi-group* and some examples and theorems, see H. Hilton, *Finite Groups* (1908), pp. 51–53.

CHAPTER II

PERMUTATIONS AND PERMUTATION GROUPS

5. Illustration. Permutations will now be taken up in order to introduce early a method commonly used for representing groups and simultaneously to introduce groups from other sources.

Take the binomial $ab-cd$, in which no two of the four quantities are to be equal, and consider the interchanges of the letters a, b, c, d that leave the value of the binomial unaltered formally. Obviously a and b may be interchanged; similarly, c and d; or both these interchanges may be carried out at the same time. Other interchanges, as a and c, would alter the value of $ab-cd$ formally.

Suppose the operation of interchanging a and b to be represented by L where $L = \begin{pmatrix} ab \\ ba \end{pmatrix}$, and similarly $M = \begin{pmatrix} cd \\ dc \end{pmatrix}$ and $N = \begin{pmatrix} ab \\ ba \end{pmatrix}\begin{pmatrix} cd \\ dc \end{pmatrix}$; symbols in which a letter in the upper line is to be replaced by the letter under it. In determining whether the elements form a group, the combination LM is naturally interpreted to mean the result of following the operation L by the operation M.

In testing to see whether the set is closed, multiplication gives

$$LM = ML = N, \quad MN = NM = L, \quad LN = NL = M.$$

But L^2 gives an element not in the set, for LL means interchanging a and b and then interchanging them again (c and d

not affected). L^2 thus leaves each letter in its original position, and therefore equals the identity I. And now, since $L^2 = M^2 = N^2 = I$ and $IL = LI = L$, etc., evidently the set L, M, N, I is closed.

Since $LL = MM = NN = I$, each element has an inverse (really itself) in the set. Finally, the associative law holds, for $(LM)N = (N)N = I$, $L(MN) = L(L) = I$, so that $(LM)N = L(MN)$; and the proof for other groupings is readily seen from the fact that the product of any two of L, M, N (in either order), always gives the third element, and the product of any one of these three by itself gives the identity. Obviously, it is unnecessary to consider cases in which the identity appears.

Since $ab-cd$ is unaltered in value by the elements of this group, it is said to be *invariant under the group.* Similarly, $a+b+c+d$, $a+b-(c+d)$, $a \cdot b \cdot c \cdot d$, $a^2 - cd + b^2$, etc., are invariant under this group. But $\frac{ac}{bd}$, $a-b-c-d$, etc., are not invariant under the group.

The elements of this group are known as permutations because each represents the operation of interchanging or permuting the letters among themselves.

6. Notation and Definitions. Some general facts about permutations will next be developed. If the letters a, b, c, d, e, f are taken and any two arrangements are used, as the one just given and the arrangement c, f, d, a, e, b, then the operation which replaces the first arrangement by the second is called a permutation. If this permutation is called L, it may be represented as

$$L = \begin{pmatrix} abcdef \\ cfdaeb \end{pmatrix},$$

which means that each letter in the first row is replaced by the letter just under it. Any order of the letters in the first row can be used provided each has under it the proper letter; thus, $\begin{pmatrix} abc \\ bca \end{pmatrix} = \begin{pmatrix} bac \\ cba \end{pmatrix}$. The identity, I, evidently is $\begin{pmatrix} abcdef \\ abcdef \end{pmatrix}$, and is included among the permutations although it does not change the letters. In general, then, the operation of replacing each of n letters by itself or another (of the n), no two letters to be replaced by the same letter, is called a **permutation.*** The number of letters included in a permutation is its **degree.** A permutation ($\neq I$) of degree two is called a **transposition.** The **degree** of a permutation group is the number of different letters in its permutations.

Evidently the total number of permutations on a given number of letters is the same as the number of ways in which the lower row can be chosen after the arrangement in the upper row is fixed once for all. By the theory of permutations the number of arrangements of n letters is $n! = 1 \cdot 2 \cdot 3 \cdot \cdots \cdot n$. Thus for two letters, a, b, there are $2! = 1 \cdot 2$ permutations, which are $\begin{pmatrix} ab \\ ab \end{pmatrix}$ and $\begin{pmatrix} ab \\ ba \end{pmatrix}$. (Note that the different arrangements are in the lower line of the symbol.) For three letters, a, b, c, there are $3! = 1 \cdot 2 \cdot 3 = 6$ arrangements and the permutations are

$$\begin{pmatrix} abc \\ abc \end{pmatrix}, \quad \begin{pmatrix} abc \\ bca \end{pmatrix}, \quad \begin{pmatrix} abc \\ cab \end{pmatrix}, \quad \begin{pmatrix} abc \\ acb \end{pmatrix}, \quad \begin{pmatrix} abc \\ bac \end{pmatrix}, \quad \begin{pmatrix} abc \\ cba \end{pmatrix}.$$

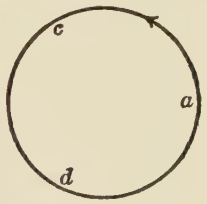
In general it may be pointed out that for n letters, the first may be replaced by any one of the n; after that is chosen, the second may be replaced by any one of the remaining $(n-1)$; after

* Some writers use *substitution*, but we shall employ this term in a broader sense (Chapter IX).

the first two are chosen, the third may be replaced by any one of the $(n-2)$ remaining; etc. Hence the total number of arrangements (permutations) is

$$n(n-1)(n-2)(n-3)\cdot \cdots \cdot 2\cdot 1 = n!.$$

Further consideration of $L = \begin{pmatrix} abcdef \\ cfdaeb \end{pmatrix}$ reveals another property. If we start with any letter (upper row) and follow the replacements in their order as indicated by the symbol, we necessarily return to the original letter. Thus in L, a is replaced by c, then c is replaced by d, and d by a. With n finite this is bound to be the case, because there are not more than n replacements and furthermore the original letter must be somewhere in the lower row. In this particular permutation, then, L permutes a, c, and d as if they were arranged on a circle and each letter were replaced by the one after it. Hence, $\begin{pmatrix} acd \\ cda \end{pmatrix}$ is called a **circular permutation, or cycle,** and is frequently written (acd) in which each letter is understood to be replaced by the one following it, and the last by the first. Evidently then $(acd) = (cda) = (dac)$. Next, if a letter not in the cycle already found, is selected, as b, a new cycle, $\begin{pmatrix} bf \\ fb \end{pmatrix} = (bf) = (fb)$, is obtained which cannot contain any of the letters in the first cycle (because in a permutation no two letters are replaced by the same letter). The one remaining letter is left unreplaced (by any letter other than itself) by the permutation L, and if this "e" is regarded as a cycle containing only one letter, L has been reduced to cycles having no letters



in common, or $L = (acd)(bf)(e)$. Similarly, any permutation may be written in cycles. A single letter cycle, as (e), is usually omitted with the understanding that such a letter is left unchanged by the permutation. We may observe that the cycles obtained from a given permutation are commutative; thus, $(acd)(bf) = (bf)(acd)$. This is because no two cycles have a letter in common.

DEFINITIONS. If the cycles of one permutation are of the same number and degree respectively as those of another permutation, the two permutations are said to be **similar.**

A **regular permutation** is one whose cycles are all of the same degree.

A **regular permutation group** is one whose elements (including the identity) take each letter over into itself and into each other letter once and only once.

From this definition we see that the order of such a group equals its degree (n). Furthermore, the degree of each permutation, as A, equals n. Since all of the powers of A are of degree n, A must be a regular permutation.

The elements of a permutation group are frequently called the permutations of the group.

7. Product of Permutations. Next, consider the meaning of the symbolic product of two permutations. If the first permutation, L, replaces a by b while the second, M, replaces b by c, evidently LM effects the replacement of a by c. This may be illustrated with permutations on the letters a, b, c.

Thus, if $L = \begin{pmatrix} abc \\ bca \end{pmatrix} = (abc)$ and $M = \begin{pmatrix} abc \\ bac \end{pmatrix} = (ab)$,

then $LM = \begin{pmatrix} abc \\ acb \end{pmatrix} = (bc)$; or this may be written

$$LM = (abc) \cdot (ab) = (bc).$$

Note that multiplication in the reverse order gives a different result. $ML = (ab) \cdot (abc) = (ac)$. Hence, (abc) and (ab) are not commutative permutations.

This method for multiplying when permutations are written in cyclical form is readily employed when more than two permutations are involved. Let us use an example to explain the method.

If $P = (abcdef)$, $Q = (be)$, $R = (afdb)$; then
$PQR = (abcdef) \cdot (be) \cdot (afdb) = (aed)(bc)$;

for first, a is replaced by b, then on to the right it is found that b is replaced by e giving us "ae"; commencing now in the left permutation with e it is observed that e is replaced by f, then on to the right we have f by d, whence PQR replaces e by d and we have thus far "aed"; next returning to $(abcdef)$ and starting with d, the replacements give d by e, e by b, then b by a; the cycle is closed and is (aed). Commencing next with a letter of $(abcdef)$ not in the product already found, say with b, we find b by c; then returning we have c by d and d by b, or that the next cycle of the product is (bc). The only letter of the permutations P, Q, R not appearing in the two cycles already found is f, and starting in $(abcdef)$ with f, we have f by a, then a by f, which shows that PQR does not replace f by a new letter.

Again, $(ade) \cdot (abc) \cdot (acbed) = I$; because a is replaced by d, then d by a, so that a is replaced by itself; then returning, d is replaced by e, e by d, so that d is replaced by itself; the next letter in the first permutation is e which is replaced by a, then a by b, and b by e, so that e is replaced by itself. The next unconsidered letter is b, which is replaced by c, then c by b, so that b remains unchanged; finally, c is replaced by a, then a by c.

Hence, the effect of the three permutations is to leave a, b, c, d, and e in their original places, or the product is I.

Attention should be called to the difference between a product of cycles having the same letter in more than one cycle, and a product of cycles having no letter in common. Thus, $(ab)(bc) = (acb)$; but $(ab)(cd)$ cannot be further simplified; and, moreover, in this case the cycles are always commutative, while in cases of the former kind some are commutative, some not.

The period of a permutation of one cycle evidently equals its degree.

The product of a permutation by itself or finding powers of a permutation is easily effected. For example, if $L = (abcd)$, $L^2 = (ac)(bd)$, $L^3 = (adcb)$, $L^4 = (a)(b)(c)(d) = I$, $L^5 = (abcd) = L$, $L^6 = L^2$, etc. If the permutation is written after itself and the method just explained is used for multiplying, it is easy to see that it would be equivalent to the following way for obtaining the square: start with some letter (say the first) and take every second letter (going around the given cycle until the cycle of the square closes), then starting with the next unused letter (if there is one) and taking every second letter, which gives a second cycle of the square. Repeat for each cycle of the given permutation. The third power is written by taking every third letter and proceeding similarly; etc.

EXERCISES

1. Reduce the following permutations to cyclical form:

$$\begin{pmatrix} abcdefgh \\ ehgfacbd \end{pmatrix}, \qquad \begin{pmatrix} abcdefgh \\ cdefghab \end{pmatrix}, \qquad \begin{pmatrix} abcdef \\ cbedfa \end{pmatrix}.$$

2. If $L = (abc)(de)$ and $M = (ae)(bd)$, find LM and ML. Does $LM = ML$?

3. Determine the group of permutations on a, b, c, d under which $ab + cd$ is invariant.

4. If $L = (abcdef)$, find L^2, L^3, L^4, L^5, L^6, L^7.

5. If $L = (abc)(de)$, find L^2, L^3, L^4, etc.

6. If $L = (abc)(def)$, find L^2, L^3, L^4, etc.

7. If $L = (ab)(cd)$, find powers of L.

8. If a permutation is made up of cycles, how is its period related to the periods of its cycles? (See preceding Exercises 4–7.)

9. Determine whether $(ab)(cd)$ is commutative with $(ac)(bd)$.

10. The various powers of $(abcde)$ form a group.* Write down the permutations of the group. What is its order and what is the period of each of its permutations?

11. Find the group given by the various powers of $(abcdef)$. What is its order and what is the period of each of its permutations?

8. Symmetric Group on Three Letters. Suppose the six possible permutations on three letters be studied. They may be changed from the two-line form given in § 6 to cyclical form; thus,

$$I, \quad (abc), \quad (acb), \quad (bc), \quad (ab), \quad (ac).$$

That each element has an inverse is seen from the products

$$(abc) \cdot (acb) = I, \quad (bc) \cdot (bc) = (ab) \cdot (ab) = (ac) \cdot (ac) = I.$$

Other products to test for the fundamental group property (closed set) are:

$$\begin{aligned} (abc) \cdot (bc) &= (ac), \\ (ab) \cdot (abc) &= (ac), \\ (ac) \cdot (ab) &= (acb), \\ (bc) \cdot (abc) &= (ab), \\ (ac) \cdot (bc) &= (abc), \\ &\text{etc.} \end{aligned}$$

That the set is closed is also obvious from the fact that it contains all possible permutations on these letters. Hence,

* Such an element is called a *generator* and is said to generate the group. More than one permutation is required to generate a non-cyclic group.

93397

the set forms a group which is of order 6 and is a non-commutative group.

9. Symmetric Group on n Letters. It is easy to show that the set of all permutations on n letters forms a group. From § 6 this group is of degree n and of order $n!$. First, the set is closed, because the product of any two permutations is itself a permutation involving no new letters; hence it is one of the permutations of the set, since the set contains all the possible permutations on these letters. Second, the associative law holds, for if L, M, N are as indicated, evidently (LM) replaces a by o, so that $(LM)N$ replaces a by x, just as is done by $L(MN)$ because L replaces a by e and (MN) replaces e by x. Third, there is an identity, $I = \begin{pmatrix} abc & \cdot & \cdot \\ abc & \cdot & \cdot \end{pmatrix}$, unique because one and only one arrangement of this kind would be in the lower row. Then $IK = KI = K$, where K is any permutation of the set.

$$L = \begin{pmatrix} a & \cdot & \cdot & \cdot & \cdot & \cdot \\ e & \cdot & \cdot & \cdot & \cdot & \cdot \end{pmatrix}$$

$$M = \begin{pmatrix} \cdot & \cdot & e & \cdot & \cdot & \cdot \\ \cdot & \cdot & o & \cdot & \cdot & \cdot \end{pmatrix}$$

$$N = \begin{pmatrix} \cdot & \cdot & \cdot & \cdot & o & \cdot \\ \cdot & \cdot & \cdot & \cdot & x & \cdot \end{pmatrix}$$

Fourth, for each permutation there is an inverse. This inverse can be obtained at once by interchanging the two rows. Thus, if $L = \begin{pmatrix} abcdef \\ efdacb \end{pmatrix}$, then $L^{-1} = \begin{pmatrix} efdacb \\ abcdef \end{pmatrix}$; for while L replaces the first arrangement by the second, L^{-1} replaces the second by the first, so that LL^{-1} leaves a, b, c, d, e, f unchanged.

Note that $L = \begin{pmatrix} abcdef \\ efdacb \end{pmatrix} = (aecd)(bf)$,

and that $L^{-1} = \begin{pmatrix} efdacb \\ abcdef \end{pmatrix} = (adce)(bf) = (dcea)(fb)$,

from which we may observe that if a permutation is in cyclical form, its inverse may be obtained by writing the letters of each cycle in opposite order (right to left).

It has been shown that the set of all permutations on n letters, $n!$ in number, forms a group. This is the group of largest order of degree n. On the six letters a, b, c, d, e, f this group would have $1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 = 720$ permutations. An invariant under this group is the polynomial $a + b + c + d + e + f$. Similarly, $a \cdot b \cdot c \cdot d \cdot e \cdot f$ or any other symmetric polynomial on these six letters is an invariant under the group. On this account such a group of $n!$ permutations is known as the **symmetric group of degree n.** Unsymmetric polynomials like $a - b + c - d + e - f$ would not be invariant under the symmetric group on the letters involved.

It might be pointed out that a rational function on n letters is **symmetric** if it is unchanged formally by any interchange among those letters (no interchange taking two different letters over into the same letter); hence, if a polynomial on n letters is invariant under the permutations of the symmetric group on these n letters, it is a symmetric polynomial. For example, if a polynomial on the letters a, b, c is formally invariant under each of the permutations I, (abc), (acb), (ab), (ac), (bc) (see § 8), it is symmetric.

In § 5, although the group was on four letters, it was not of order $1 \cdot 2 \cdot 3 \cdot 4 = 24$, but of order 4. Evidently, then, groups can be formed which consist of only a part of the $n!$ permutations of the symmetric group on those letters. A group whose elements are thus included in a second group is known as a **subgroup** of the second group.

EXERCISES

1. Show an easy way to write the inverse of a permutation if the permutation is written (*i*) in two-line form; (*ii*) in cyclical form.

2. Prove that an element of a permutation group and its inverse are of the same period and of the same degree.

3. Write in cyclical form all the permutations of the symmetric group on the four letters a, b, c, d.

4. Prove: A symmetric group of degree $m (m > 2)$ contains as subgroups all symmetric groups of degrees less than m.

5. A symmetric group of degree $n (n > 2)$ contains a subgroup of order n.

6. Show that the set of all permutations on the n letters a, b, c, etc., under which a given polynomial on these letters is formally invariant, forms a group.

7. Prove that if a polynomial on a, b, c is invariant under the transpositions (ab), (ac), (bc), it is a symmetric polynomial. Generalize this statement.

10. Theorems on Permutations.

THEOREM 1. *Any permutation can be expressed as the product of transpositions.*

Since any permutation can be written as the product of cycles no two of which have a letter in common, it is only necessary to show the theorem true for circular permutations. This is obvious from the following identity:

$$(abcde \cdots l) \equiv (ab)(ac)(ad)(ae) \cdot \cdots \cdot (al).$$

Since $(ab)(ac) = (ac)(bc) = (bc)(ab)$, evidently a permutation (of degree > 2) can be expressed as a product of transpositions in more than one way using only its own letters.

If a permutation A on n letters is equal to the product of two or more permutations involving no other letters, we may say that A is factored into these permutations.

THEOREM 2. *The number of transpositions into which a given permutation can be factored on its own letters is always even or else always odd.*

Suppose the given permutation, A, is on the n letters $a, b, c, d, \cdots, l$. Any transposition on these letters changes the sign of the determinant D following, because it interchanges two rows.

$$D \equiv \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 \\ a & b & c & \cdots & l \\ a^2 & b^2 & c^2 & \cdots & l^2 \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ \cdot & \cdot & \cdot & \cdots & \cdot \\ a^{n-1} & b^{n-1} & c^{n-1} & \cdots & l^{n-1} \end{vmatrix} *$$

Hence, an odd number of transpositions changes D into $-D$, an even number leaves D unaltered; and conversely. Since the various sets of transpositions into which A is factored must affect D just as A does, the property stated in the theorem must hold.

DEFINITIONS. A permutation is said to be **positive** or **negative** † according as it factors into an even or an odd number of transpositions, respectively.

If A and B are elements (permutations), the element $B^{-1}AB$ is the **transform** of A by B, while $A^{-1}B^{-1}AB$ is the **commutator** of A and B. That is, if $BAC = AB$, C is the commutator of A and B and $C = A^{-1}B^{-1}AB$.

If $B^{-1}AB = K$, B is said to **transform A into K**; if $B^{-1}AB = A$, A is said to be **invariant under B**, and A and B are **commutative.**

A set of elements is said to be **invariant under an element B,**

* Called the *determinant of Vandermonde* because he first (1770) studied it.

† Some authors use *even* and *odd* instead of *positive* and *negative*.

if B transforms them among themselves only. It is not necessary that B transform each element of the set into itself.

A subgroup H is said to be **invariant** in its group G if every element of G transforms H into itself.*

COROLLARY 1. *There is at least one positive permutation in each permutation group.* Because I is in every group and I is positive.

COROLLARY 2. *The product of permutations is positive or negative according as the total number of negative permutations among the factors is even or odd, respectively.*

COROLLARY 3. *The inverse of a permutation is positive or negative according as the permutation itself is positive or negative.*

THEOREM 3. *If a permutation T is formed from a permutation S by replacing each letter (of S) by the nth one after it in its cycle, where n is a positive integer, then $T = S^n$.*

The truth of this theorem is obvious from the method given in § 7 for writing powers of a permutation.

THEOREM 4. A THEOREM OF NETTO'S.† *Given that S is the circular permutation $(abcd \cdots m)$. The only permutations on the letters $a, b, c, \cdots, m$ which are commutative with S are its own powers.*

Suppose R is a permutation on the letters $a, b, c, \cdots, m$ but is not a power of S. From the preceding Theorem if R replaces a by the nth letter after it in S, not every other letter in R is replaced by the nth letter after it in S. Suppose b, for convenience, is replaced by the kth letter after it, where $k \neq n$. Then in the product RS, a is replaced by the $(n+1)$th letter after it, while in SR, a is replaced by the $(1+k)$th letter after it. Since $k \neq n$, $RS \neq SR$. Hence, the theorem is proved.

* *Self-conjugate* subgroup is used occasionally for *invariant* subgroup.

† Crelle's *Journal für die reine und Angewandte Mathematik*, vol. 103 (1888), p. 323.

THEOREM 5. *The transform of a permutation S by a permutation T may be written by displacing each letter of S by the letter by which it is replaced in T.*

It will be sufficient to show this for one cycle of S, since for other distinct cycles the method would be the same.

Let $S = (abcd) = \begin{pmatrix} abcd \\ bcda \end{pmatrix}$, and $T = \begin{pmatrix} abcd \cdots k \cdot \\ xyzw \cdots u \cdot \end{pmatrix}$; then it is to be proved that $T^{-1}ST = (xyzw)$.

Now
$$T^{-1}ST = \begin{pmatrix} xyzw \cdots u \cdot \\ abcd \cdots k \cdot \end{pmatrix}\begin{pmatrix} abcd \\ bcda \end{pmatrix}\begin{pmatrix} abcd \cdots k \cdot \\ xyzw \cdots u \cdot \end{pmatrix}$$
$$= \begin{pmatrix} xyzw \cdots u \cdot \\ bcda \cdots k \cdot \end{pmatrix}\begin{pmatrix} abcd \cdots k \cdot \\ xyzw \cdots u \cdot \end{pmatrix}$$
$$= \begin{pmatrix} xyzw \\ yzwx \end{pmatrix} = (xyzw). \qquad Q.E.D.$$

From the second line preceding or from the theorem itself, if T replaces letter k by u but k does not appear in S, then u will not appear in $T^{-1}ST$.

COROLLARY 1. *The permutations S and $T^{-1}ST$ are similar, and hence of the same period and degree, and both positive or else both negative.*

COROLLARY 2. *If the permutations S and X are similar, a permutation T can always be found such that $T^{-1}ST = X$.*

For, writing the cycles of X under the corresponding ones of S gives T immediately in two-line form.

EXERCISES

1. Show that the identity is a positive permutation.

2. Prove that an element of a permutation group and its inverse are both positive or else both negative. (*Cf.* p. 18, Ex. 2.)

3. Prove: The commutator of two permutations is positive.

4. Elements A and B of a group are commutative, (*i*) if A equals its transform by B, or (*ii*) if their commutator is the identity; and conversely.

5. Transform all the elements of the group

$$I, (abc), (acb), (ab), (ac), (bc),$$

(*i*) by (ab); (*ii*) by (acb); (*iii*) by $(ax)(by)(cz)$.

6. If p is a prime integer, show that the symmetric group of degree p contains exactly $(p-1)!$ elements of period p and $(p-2)!$ subgroups of order p.

7. Show that the following definition and the one in § 9 are equivalent. A rational function on n letters is symmetric if it is unchanged formally by every interchange of two of those letters.

8. Prove Theorem 2 of § 10 by using the following product instead of Vandermonde's determinant D:

$$\begin{aligned} P = (a-b)\cdot(a-c)\cdot(a-d)\cdot\cdots\cdot(a-l) \\ \cdot(b-c)\cdot(b-d)\cdot\cdots\cdot(b-l) \\ \cdot(c-d)\cdot\cdots\cdot(c-l) \\ \cdot\cdots\cdot\cdots \\ \cdot(k-l). \end{aligned}$$

11. Some General Theory of Finite Groups.

Cayley's Multiplication Table of a Group.* An easy way to explain the make-up of a multiplication table is to construct one for some group, as the group of § 2. The table may be arranged as a square array as follows:

I	A	B	P	Q	R
P	R	Q	I	B	A
A	B	I	Q	R	P
Q	P	R	A	I	B
B	I	A	R	P	Q
R	Q	P	B	A	I

I	A	B	P	Q	R
B	I	A	R	P	Q
A	B	I	Q	R	P
P	R	Q	I	B	A
Q	P	R	A	I	B
R	Q	P	B	A	I

The table is made up of products; first factor is from the first column, second factor from the first row (or vice versa throughout), and the product is written where the row and column of the first and second factors, respectively, intersect. If any element is non-commutative in its group, it is important to take the

* If the group is of order n, its multiplication table is really a "Latin square of order n."

factors in the same order throughout. The elements do not have to be in the same order in the first column as in the first row. In the right-hand table the elements are arranged to make the identity appear in the principal diagonal.

Since the product of every element by every element of a given group appears in its multiplication table, all the abstract properties of the group (*i.e.*, properties which are independent of how its elements are represented) are embodied in the table. Hence, a group is abstractly determined by its multiplication table, or

DEFINITION. If a one-to-one correspondence of the elements of one group with those of another group can be found which holds throughout in their multiplication tables, *the two groups are abstractly identical.*

Thus, if certain elements of the first group G form a subgroup, the corresponding elements of the second group G' will form a subgroup; to the commutator of any two elements of G will correspond the commutator of the two corresponding elements of G'; etc.

To illustrate, suppose the following groups first paired off as indicated and then their multiplication tables formed as shown. ($i = \sqrt{-1}$.)

G	G'
$I = 1$	I
i	$(abcd)$
-1	$(ac)(bd)$
$-i$	$(adcb)$

1	i	$-i$	-1
i	-1	1	$-i$
-1	$-i$	i	1
$-i$	1	-1	i

I	$(abcd)$	$(adcb)$	$(ac)(bd)$
$(abcd)$	$(ac)(bd)$	I	$(adcb)$
$(ac)(bd)$	$(adcb)$	$(abcd)$	I
$(adcb)$	I	$(ac)(bd)$	$(abcd)$

The products everywhere correspond; *e.g.*, i (first column) times -1 (first row) gives $-i$, and the correspondence is $(abcd)$ times $(ac)(bd)$ equals $(adcb)$.

Usually there is more than one way that the pairing can be set up between the two given groups. Usually, also, there are pairings, even between abstractly identical groups, which will not hold between the corresponding elements of their multiplication tables. Thus, if we had tried having i of G correspond to $(ac)(bd)$ of G', etc., not all the products would correspond (note for example the second columns).

G	G'
$I = 1$	I
i	$(ac)(bd)$
-1	$(abcd)$
$-i$	$(adcb)$

1	i	$-i$	-1	I	$(ac)(bd)$	$(adcb)$	$(abcd)$
i	-1	1	$-i$	$(ac)(bd)$	I	$(abcd)$	$(adcb)$
-1	$-i$	i	1	$(abcd)$	$(adcb)$	I	$(ac)(bd)$
$-i$	1	-1	i	$(adcb)$	$(abcd)$	$(ac)(bd)$	I

THEOREM 1. *The order of a subgroup is a factor of the order of its group.*

This is sometimes called Lagrange's theorem although both Abbati and Galois seem to have been nearer the idea and proof of the theorem as here stated.*

To prove the theorem let the subgroup H be of order h and its elements be $I, A, B, \cdots, F$, and let the order of the whole group G be g.

If X is some element not in the subgroup H, then the following $2h$ elements are distinct and are all in G:

$$I, \quad A, \quad B, \quad \cdots, \quad F,$$
$$X, \quad AX, \quad BX, \quad \cdots, \quad FX;$$

* Carmichael, R. D., *Bull. Am. Math. Soc.*, vol. 27 (1921), p. 474.

because $AX = FX$ would give $A = F$ or $AX = B$ would give $X = A^{-1}B$, either of which is impossible.

If the given group contains an element not in the array, say Y, then

$$IY, \quad AY, \quad BY, \quad \cdots, \quad FY$$

would all be distinct among themselves and from any element in the first or second row. This last is because if $AY = BX$, then $Y = A^{-1}BX$ and Y would be in the second line, which is contrary to assumption. For a finite group, evidently this process must end and must end with an integral number of complete rows. Hence h is a factor of g.

COROLLARY 1. *The period of any element of a group divides the order of the group.*

COROLLARY 2. *If H is a subgroup of G,*

$$G \equiv H + H \cdot X + H \cdot Y + \cdots + H \cdot Z,$$

where each of $X, Y, \cdots, Z$ is an element of G not already in H nor in products obtained before it is introduced.

$H \cdot X$ means the product of each element of the subgroup H by the element X. $H \cdot X, H \cdot Y, \cdots, H \cdot Z$ are known as co-sets of G as regards H.* It is easy to prove that the co-set $H \cdot U$ contains exactly the same elements if U is replaced by any other element in the co-set.

DEFINITION. The index of a subgroup in a given group is the quotient of the order of the latter by the order of the former.

THEOREM 2. *A subgroup of index 2 is invariant under its group.*

* These are sometimes called *right co-sets*, and $X_1 \cdot H, Y_1 \cdot H, \cdots, Z_1 \cdot H$ called *left co-sets*.

Let the elements of the subgroup H be represented by I, A, B, $\cdots$, F, which are half of the elements of the group G. If H is not invariant under G, some element, say X, outside of H must transform some element of H into one of the elements of G outside H; that is, into one of the elements of the co-set IX, AX, BX, $\cdots$, FX. Suppose then that $X^{-1}AX = FX$. Simplifying this gives $AF^{-1} = X$, which requires X to be in H. Thus, the contrary of the theorem is impossible.

EXERCISES

Prove the following statements:

1. Transforming all the elements of a group by one of its elements gives all the elements in some order. (*Cf.* p. 22, Ex. 5.)

2. The transforms of the elements of a group by any element form a group.

3. All the elements of a group that are individually invariant under some element of the group, form a subgroup.

4. All the elements of a group that are individually invariant under each of the elements of the group, form an invariant subgroup. This invariant subgroup is called the **central** of the given group.

5. DEFINITION. A commutative group is frequently called an **abelian group.*** If some two elements of a group are not commutative, the group is said to be **non-abelian.** Prove that a group is abelian if and only if it is identical with its central.

6. The central of a symmetric group of degree greater than two is the identity.

7. What are the co-sets of the symmetric group on a, b, c, d, with respect to the subgroup

$$I,\ (ab)(cd),\ (ac)(bd),\ (ad)(bc),\ (abcd),\ (bd),\ (adcb),\ (ac)?$$

(*Cf.* p. 18, Ex. 3.)

8. If $H \cdot U$ is a co-set of a group G, prove that $H \cdot U \equiv H \cdot CU$, where C is any element of the subgroup H.

9. Construct a multiplication table for the permutation group of order eight given in Exercise 7 preceding.

* Named for Abel (1802–1829) because he first made a general study of these groups in connection with the theory of the algebraic equation.

10. If a group contains no elements of period greater than 2, prove that it is an abelian group.

11. Prove that two cyclic groups of order g are abstractly identical. Hint. Construct multiplication tables.

12. Prove: A necessary and sufficient condition that a set of group elements which is not itself a group be a right co-set, is that it involve at least one element such that if every element of the set is multiplied on the right by the inverse of that element, the resulting products constitute a group.*

12. Some Theorems on Permutation Groups.

THEOREM 1. *The positive elements of a permutation group either comprise the entire group or else form an invariant subgroup of half the order.*

From the Corollaries of Theorem 2 in § 10, the set of positive permutations is seen to form a group. If not all are positive, suppose $I, A, B, \cdots, K$ are positive and distinct, and that $W, X, \cdots, Z$ are negative and distinct. From a Corollary just referred to, $WI, WA, \cdots, WK$ are negative; they are distinct likewise, for if $WA = WK$, then $A = K$ which is contrary to the supposition that these permutations are distinct. Hence, there are at least as many negative permutations as positive ones in the group. Similarly, $WW, WX, \cdots, WZ$ are positive and distinct. Hence, there are at least as many positive permutations as negative ones in the group. The theorem then follows, because a subgroup of index 2 is invariant in its group (§ 11, Theorem 2).

Again, since (ab) is a negative permutation, the following is evident.

THEOREM 2. *The positive permutations of a symmetric group of degree n, $n > 1$, form a group of order $n!/2$.*

* The word "right" may be replaced throughout by the word "left." This theorem is due to Professor Miller. See *Bulletin of the American Mathematical Society*, vol. XXXIV (1928), p. 307.

This group is known as the **alternating group** of degree n. Its permutations do not change the sign of the determinant in § 10, or it may be said to consist of all permutations on the n letters under which the determinant is invariant.

THEOREM 3. *If the elements of a group are written as circular permutations, all those not containing specified letters form a subgroup.*

These permutations will fulfill the group requirements: the identity is in the set, the product of any two is in the set, etc.

By use of the multiplication table Cayley's theorem * will next be proved.

THEOREM 4. *Any finite group of order n can be represented as a regular permutation group of degree n.*

Suppose $I, \cdot\cdot, B, \cdot\cdot, D, \cdot\cdot, N$ are the elements of the given group. Let a multiplication table of it be formed as follows (Table 1):

I	B	D	N
B	B^2	DB	NB
D	BD	D^2	ND
N	BN	DN	N^2

Table 1

I'	B'	D'	N'
B'	B'^2	$D'B'$	$N'B'$
D'	$B'D'$	D'^2	$N'D'$
N'	$B'N'$	$D'N'$	N'^2

Table 2

Each row represents the elements of the group in some order (p. 7, Ex. 4), and no row after the first gives an element in

* *Philosophical Magazine*, vol. 7 (1854), p. 40.

the same column it occupies in any other row (for example, DB could not equal DN).

Consider now the set of n permutations which replace the arrangement in the first row by the arrangements in the n rows; thus,

$$B' = \begin{pmatrix} I & \cdot\cdot & B & \cdot\cdot & D & \cdots & N \\ B & \cdot\cdot & B^2 & \cdot\cdot & DB & \cdots & NB \end{pmatrix},$$

$$D' = \begin{pmatrix} I & \cdot\cdot & B & \cdot\cdot & D & \cdots & N \\ D & \cdot\cdot & BD & \cdot\cdot & D^2 & \cdots & ND \end{pmatrix}.$$

It will now be shown that these n permutations are regular and form a group; then, by means of its multiplication table, that this group is abstractly identical to the given group.

If B is of period m, B' is of period m and regular; for B' would replace D by DB, DB by DB^2, DB^2 by DB^3, $\cdots$, DB^{m-1} by D, which is a cycle of period m. Following the same reasoning with a letter not in this cycle (if there be such), B' would be seen to be made up of cycles each of degree m; hence, B' is of period m and regular.

The set will be a group if closed (*cf.* p. 7, Ex. 10). It will now be shown that $B'D'$ is in the set. Following B' by D' gives

$$B'D' = \begin{pmatrix} I & \cdot\cdot & B & \cdot\cdot & D & \cdots & N \\ BD & \cdot\cdot & B^2D & \cdot\cdot & DBD & \cdots & NBD \end{pmatrix},$$

which is one of the set; because, since BD is in the original group, BD, $\cdot\cdot$, B^2D, $\cdot\cdot$, DBD, $\cdot\cdot$, NBD is one of the rows in Table 1.

Furthermore, if I' is made to correspond to I, B' to B, $\cdots$, N' to N, the multiplication Tables 1 and 2 will correspond element to element throughout: for B' and B are of the same period, $\cdots$, N' and N are of the same period; and from what has just been developed, $B'D'$ would correspond to BD.

Hence, by the definition of § 11 the two groups are abstractly identical.

EXAMPLE. Table 1 following is a multiplication table for the symmetric group on the three letters x, y, z. In each row the common multiplier is used on the right of each of the six elements. (How does this method compare with that used in § 11? If a group is abelian, the two multiplication tables resulting from left multiplication and right multiplication are identical.) Next, a single letter is used for each element as shown between the two tables, and Table 1 thus re-written as Table 2.

I	(xyz)	(xzy)	(xy)	(xz)	(yz)
(xy)	(yz)	(xz)	I	(xzy)	(xyz)
(xyz)	(xzy)	I	(xz)	(yz)	(xy)
(xz)	(xy)	(yz)	(xyz)	I	(xzy)
(xzy)	I	(xyz)	(yz)	(xy)	(xz)
(yz)	(xz)	(xy)	(xzy)	(xyz)	I

Table 1

I	$-a$
(xyz)	$-b$
(xzy)	$-c$
(xy)	$-d$
(xz)	$-e$
(yz)	$-f$

Correspondence

a	b	c	d	e	f
d	f	e	a	c	b
b	c	a	e	f	d
e	d	f	b	a	c
c	a	b	f	d	e
f	e	d	c	b	a

Table 2

Corresponding to the permutations on x, y, z, we get from Table 2 the following permutations on a, b, c, d, e, f:

$$I - \begin{pmatrix} abcdef \\ abcdef \end{pmatrix}, \text{ or } I$$

$$(xy) - \begin{pmatrix} abcdef \\ dfeacb \end{pmatrix}, \text{ or } (ad)(bf)(ce)$$

$$(xyz) - \begin{pmatrix} abcdef \\ bcaefd \end{pmatrix}, \text{ or } (abc)(def)$$

$$(xz) - \begin{pmatrix} abcdef \\ edfbac \end{pmatrix}, \text{ or } (ae)(bd)(cf)$$

$$(xzy) - \begin{pmatrix} abcdef \\ cabfde \end{pmatrix}, \text{ or } (acb)(dfe)$$

$$(yz) - \begin{pmatrix} abcdef \\ fedcba \end{pmatrix}, \text{ or } (af)(be)(cd)$$

That this new set makes up a group abstractly identical with the given group could be verified by forming the multiplication table for the six new elements starting with the elements as they pair off with those on x, y, z, and then comparing it with Table 1. Thus, corresponding to the product of (xy) and (xyz), which is (xz), we would expect to find the product of the corresponding elements $(ad)(bf)(ce)$ and $(abc)(def)$, which is $(ae)(bd)(cf)$. This checks, for (xz) and $(ae)(bd)(cf)$ correspond.

EXERCISES

1. Write the alternating group on the four letters a, b, c, d. (*Cf.* p. 18, Ex. 3.)

2. Show that the elements of the symmetric group on the four letters a, b, c, d which do not replace b by another letter form a subgroup. What group is it?

3. Given the group I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$, (abc), (acb), (abd), (adb), (acd), (adc), (bcd), (bdc), in which are the subgroups: (*i*) I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$, and (*ii*) I, (abc), (acb). Determine for each subgroup whether it is invariant or not under the given group.

4. Show that the elements of the group of order 12 in Exercise 3 which omit the letter c form a subgroup. Is this subgroup invariant under the given group?

5. Prove that the alternating group of degree n is an invariant subgroup of the symmetric group on the n letters.

6. Prove: All the elements of odd period in the symmetric group of degree n are in the alternating group of degree n. Hint. § 10, Th. 2, Cor. 2.

7. If a permutation group on n letters contains all the transpositions on those letters, show that it is the symmetric group of degree n. Hint. Use the identity of § 10, Theorem 1.

8. Take a single letter to represent each element of the octic group I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$, $(abcd)$, (bd), $(adcb)$, (ac); construct its multiplication table on these new letters (*cf.* p. 26, Exer-

cise 9); and therefrom write a regular group of degree 8, abstractly equivalent to the given group.

ADDITIONAL EXERCISES

1. *Jordan's Theorem.* G is a regular permutation group of order and degree n. Prove that all the permutations of degree n on the same letters which are commutative with each of the elements of G, form a group which is abstractly identical with G. *Cf.* Burnside, *Theory of Groups* (1911), § 20.

2. If a group G is separated into co-sets as regards a subgroup H, so that $G \equiv H + H \cdot X + H \cdot Y + \cdots + H \cdot Z$,
show that $G \equiv H + X^{-1} \cdot H + Y^{-1} \cdot H + \cdots + Z^{-1} \cdot H$.
Cf. Hilton, *Finite Groups* (1908), p. 59.

3. Prove that any positive permutation can be factored into cycles of degree 3. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), p. 18.

CHAPTER III

PERMUTATION GROUPS, CONTINUED: TRANSITIVITY AND PRIMITIVITY

13. Illustration and Definitions. In the present chapter some additional theory on permutation groups will be discussed, particularly transitivity and primitivity.

Consider the following groups each written on the four letters a, b, c, d.

$$I, \quad (ab)(cd), \quad (ac)(bd), \quad (ad)(bc);$$
$$I, \quad (ab)(cd), \quad (ab), \qquad (cd).$$

In each group we see that the elements other than I are of period 2; the product of any two elements of period 2 is the third element of period 2; the elements are commutative; and the group is of order 4. The groups are accordingly identical abstractly (§ 11). This abstract group is sometimes called the **four-group.** As permutation groups, however, the two groups are quite different. In the first one, permutations replace each of the letters of the group by each of the other letters (and by itself). Such a permutation group is known as a **transitive group.** In the second it is not true that each letter is replaced by every other letter (and itself) by the permutations, and hence this group is said to be **intransitive.**

14. Elementary Theorems on Transitive Groups. From the proof of Theorem 4 in § 12 evidently any finite group of order n can be represented as a transitive permutation group of degree n. Again, since there must be at least as many elements in a transitive group as there are different letters in its permutations, its degree is not greater than its order. Also, since a

permutation of prime period p must contain at least one cycle of degree p and cycles of no other degree (p. 15, Ex. 8), obviously a cyclic group of prime order p cannot be represented as a permutation group on fewer than p letters; if on p letters, it is regular and transitive; if on more than p letters, the degree is a multiple of p and the group is intransitive.

That the degree of a transitive group may be less than its order is illustrated by the following which abstractly is known as the *octic group*:

$$I,\ (ac)(bd),\ (abcd),\ (adcb),\ (ac),\ (bd),\ (ab)(cd),\ (ad)(bc).$$

A glance at this group suggests

THEOREM 1. *If in a transitive group on the h letters $a, b, c, \cdots, n$, exactly m permutations replace a certain letter by another letter, every letter is replaced by each of the letters exactly m times.*

In proving this it will first be shown that if a is replaced by b in exactly m different permutations of the group, it is replaced by every letter m times. Without less of generality it may be supposed that no letter is replaced by another more times than a is replaced by b. Let a rectangular array of the elements be built up, the first column being the m distinct permutations replacing a by b. Since the group is transitive, there must be a permutation replacing b by c, as $(bc \cdot \cdot)$. Multiplying on the right each of the m permutations of the first column by $(bc \cdot \cdot)$ gives m different permutations for the second column each replacing a by c; similarly m different permutations replace a by d; etc. (including a by a). Hence a is replaced by each of the h letters exactly m times.

Taking inverses in the first column would give m different permutations replacing b by a. From the preceding paragraph

then, b is replaced by each of the h letters m times; etc., and the theorem is established.

Furthermore, the rectangular array was so set up that it must use each element of the group once and only once; hence, $h \cdot m$ must equal the order of the group, or

THEOREM 2. *The degree of a transitive permutation group is a factor of its order.*

Again, since in the group each of the h letters is replaced by other letters $(h-1)m$ times, and these replacements and no others are written in the circular permutations, the total number of letters is $h(h-1)m$. But it was just pointed out that the order of the group is $h \cdot m$. Hence, the following, a minor theorem of Frobenius, is established:

THEOREM 3. *The average number of letters per permutation in a transitive permutation group is one less than the degree of the group. (Permutations are in circular form.)*

EXERCISES

Six permutation groups are here given.

1) I, $(abcd)$, $(ac)(bd)$, $(adcb)$.
2) I, $(ab)(cd)$, $(ab)(ef)$, $(cd)(ef)$.
3) I, (abc), (acb), (ab), (ac), (bc).
4) I, $(abcdef)$, $(ace)(bdf)$, $(ad)(be)(cf)$, $(aec)(bfd)$, $(afedcb)$.
5) I, (abc), (acb), $(ab)(de)$, $(ac)(de)$, $(bc)(de)$.
6) I, $(abc)(de)$, $(acb)(de)$, (abc), (de), (acb).

1. For each of these six groups determine order, degree, and whether transitive or intransitive.

2. Verify each of the three theorems of § 14 in each transitive group in the given list.

3. Determine whether the symmetric and alternating groups of degree n are transitive or intransitive.

4. How many letters *in toto* are required to write the symmetric group of degree n in cyclical form? The alternating group of degree n?

5. Prove: If in a transitive group on h letters, exactly m permutations replace a certain letter by another letter, every letter is omitted by exactly m permutations.

6. The class of a permutation group is the number of letters in any of its (circular) permutations of lowest degree (excepting the identity). What is the class of a symmetric group of degree > 2? Of an alternating group of degree > 2? Of each of the six groups in the list heading these Exercises?

7. Prove: A transitive group of degree n contains at least $n - 1$ permutations of degree n. Hint. Apply Frobenius' minor theorem of this Section.

8. If a transitive group of degree n contains n or more permutations of degree n, show that it contains permutations of degree less than $n - 1$.

9. Given a permutation group G of degree n. Prove: (i) if all the elements of degree n in G do not generate G, they generate an invariant subgroup H; and (ii) if G and H are transitive, each element of G not in H is of degree $n - 1$. Note. By use of Exercise 5, p. 55, it can be proved that, if G is transitive, the subgroup H is transitive.

10. Prove: If a transitive group G of degree n contains no permutation of degree $n - 1$, then G is generated by its permutations of degree n.

15. Conjugate Set of Elements. Before proceeding with the main topics of the Chapter some additional definitions and theory should be introduced. Permutations are ideal agents for explaining conjugates, although the concept, as will be seen from the definition, is one of abstract groups as well as of permutation groups.

Consider the alternating group of degree four: I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$, (abc), (acb), (abd), (adb), (acd), (adc), (bcd), (bdc). In this group, if $(ab)(cd)$ is transformed by (acd), the result is $(ad)(bc)$; if now the process is repeated (that is, $(ad)(bc)$ is transformed by (acd), or what amounts to the same thing, $(ab)(cd)$ is transformed by the square of (acd)), the result

is $(ac)(bd)$; on transforming again, the original $(ab)(cd)$ is obtained. The elements $(ab)(cd)$, $(ad)(bc)$, $(ac)(bd)$ are said to be *conjugates under* (acd). If instead of (acd) all the elements of the group were used, the set of conjugates in this group would still be $(ab)(cd)$, $(ad)(bc)$, $(ac)(bd)$; although usually the set of conjugates under one element is not the same as the set under the group. In general, if transforming an element A_1 of a given group by each of the elements of the group gives the m distinct elements $A_1, A_2, \cdots, A_m$, then these elements are said to be **conjugates of A_1** in the group, or to be a **conjugate set of elements** in the group. The equivalence of these two designations will be proved.

First, *if exactly h elements of the given group transform A_1 into itself, exactly h transform A_1 into A_2.* For, if B transforms A_1 into A_2, the product of any one of those h elements and B gives an element which transforms A_1 into A_2. There are no others, for suppose $C^{-1}A_1C = A_2$, or $A_1 = CA_2C^{-1}$. Since some element (X) of the group can be found such that (p. 7, Ex. 4) $XC = B$, or $C = X^{-1}B$, evidently

$A_1 = X^{-1}BA_2B^{-1}X = X^{-1}A_1X$ (because $A_1 = BA_2B^{-1}$), which (because $C = X^{-1}B$) shows that C is the product of an element commutative with A_1 and of B.

Second, if an element transforms A_1 into A_2, its inverse transforms A_2 into A_1; hence, *just as many elements transform A_2 into A_1 as transform A_1 into A_2.*

Noting now that A_2 is transformed into itself by the h products of the h different elements which transform A_1 into A_2 and of B^{-1}, and by no other elements, and then applying to element A_2 the first observation, the following results:

THEOREM 1. *If in a given group the elements $A_1, A_2, \cdots, A_m$ are the conjugates of A_1, they are likewise the conjugates of A_2.*

This establishes the equivalence of the two designations of conjugacy of elements in a group. Furthermore, since every element of the group must transform A_1 into some one of the conjugate set, by the two observations the elements of the group could be arranged in a rectangular array, from which the following would be obvious.

THEOREM 2. *If an element A of a group is transformed into itself by exactly h elements of the group and A has m conjugates in the group, then the order of the group equals $h \cdot m$.*

On referring to the alternating group of degree 4 again, it will be found that under $(ac)(bd)$ the elements (adb) and (bdc) are conjugates. Also, under (acd) the element $(ab)(cd)$ will be found to have three conjugates. This suggests the question: If A and B are elements of a group, how many conjugates has A under B? Obviously, to determine this number there must be knowledge of the relations between the given elements. In finding the set of conjugates, A would be transformed by B, by B^2, by B^3, and the process continued until A was again obtained; that is, until $B^{-n}AB^n = A$. This might be formally stated as follows:

THEOREM 3. *If B^n is the lowest positive integral power of B commutative with A, then A has n conjugates under B.*

This is because succeeding powers of B would reproduce the set. It might be noted that n is not greater than the period of B, in fact n must be a factor of the period of B.

THEOREM 4. *The order of a group G equals the sum of the number of elements in each of all its complete sets of conjugate elements.*

Since no element belongs in more than one set of conjugate

elements in G and some (as the identity) may be invariant, this theorem merely states that all the elements of G can be arranged in sets of conjugates. If G is of order n and there are m_1, m_2, etc., in the successive sets after the central whose order is c, we have

$$n = c + m_1 + m_2 + \text{etc.}$$

Note that c and each m_i divides n.

16. Conjugate Set of Subgroups. Suppose the subgroup I, (abc),(acb) of the alternating group of degree four used in the preceding section to be transformed by another element of the group, say by (abd). The following three subgroups and no more are obtained by successive transformations, and are said to form a *conjugate set of subgroups* (or groups) *under* (abd):

I	I	I
(abc)	(bdc)	(acd)
(acb)	(bcd)	(adc).

Under $(ad)(bc)$ there are but two subgroups in the conjugate set.

I	I
(abc)	(bdc)
(acb)	(bcd).

It is interesting to find into what subgroups I, (abc), (acb) would be transformed by all the elements of the group. The set of different subgroups obtained by transforming a given subgroup of a given group G by all the elements of G is known as a **conjugate set of subgroups in G.** The subgroups of such a set are said to be the conjugates of any one subgroup of the set.

EXERCISES

1. In the alternating group of degree four given in § 15, find (*i*) the conjugates of the subgroup I, $(ab)(cd)$ in the group; (*ii*) the conjugates of the subgroup I, (abc), (acb) in the group.

2. What are the conjugates of element (abc) in group (6) on p. 35?

3. How many conjugates has any element in a cyclic group? In any commutative (abelian) group? Why?

4. What are the conjugates of (abc) in group (5) on p. 35?

5. In the symmetric group on the four letters a, b, c, d, find the conjugates of (i) the four-group I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$; (ii) the four-group I, $(ab)(cd)$, (ab), (cd).

6. Find the conjugates of the octic group given in § 14 in the symmetric group on the letters a, b, c, d.

7. In a permutation group G, if a subgroup H is such that there is no other subgroup whose generating elements are respectively similar to the generating elements of H, what can be said about the conjugates of H in G?

17. Theorems Involving Conjugates. Evidently all the elements of a group which transform one of its subgroups into itself, themselves form a subgroup. (*Cf.* p. 26, Exercise 3.) For, if elements A_1 and A_2 each transform subgroup K into itself, A_1A_2 likewise does. If A_i, $i = 1, \cdots, m$, and no other elements of the group G transform K into itself, and if B transforms K into K_1, then there are exactly m elements, BA_i, which transform K into K_1. If G has an element C besides A_i, and BA_i, $i = 1, \cdots, m$, evidently it (C) must transform K into K_2. There will be exactly m such elements, CA_i; etc. Thus the elements of G separate into sets, one to each of the subgroups conjugate to K, each set containing m elements, and no elements of G repeated. Hence:

THEOREM 1. *The number of the subgroups in a conjugate set is a factor of the order of the group.*

COROLLARY. *The number of the elements in a conjugate set is a factor of the order of the group.*

THEOREM 2. *If in a group G the subgroup K is one of a con-*

jugate set of h subgroups, all the elements of G that transform K into itself form a subgroup of index h in G.

The Theorem 3 of § 12 can now be extended to read

THEOREM 3. *In a group G of degree h all the permutations that leave one letter fixed form a subgroup K. If G is transitive and K of degree h − 1, K is one of a conjugate set of h subgroups and is of index h in G.*

For if G is on h letters, a, b, c, etc., and K is the subgroup formed by all the permutations omitting a, K can be transformed into $h - 1$ conjugates by elements replacing a by b, a by c, etc., respectively. Since G is transitive, such elements occur in it and are not in K. Each of these h conjugates omits a letter found in the others of the set; hence the h conjugates are distinct. However, a pair of the conjugates may have some elements in common. All the elements common to two groups form what is called their **cross-cut.**

Any element of G outside K must contain $\widehat{a}$ and hence cannot be commutative with K. Accordingly, by the preceding Theorem, K is of index h in G.

COROLLARY. *The permutations common to the subgroups of a conjugate set form an invariant subgroup.*

From the fact that a subgroup either is invariant or has conjugates under its group, the following is obvious.

THEOREM 4. *If K is an invariant subgroup (not the identity) in a transitive group of degree n, K is of degree n.*

The following fundamental theorem by Miller has to do with the conjugates of a cycle in a permutation group whether the group is transitive or intransitive: *

THEOREM 5. *If the cycle* $(a_1 a_2 \cdots a_r)$ *appears in exactly q*

* Miller, G. A., *American Journal of Mathematics*, vol. 44 (1922), p. 122.

different elements of a permutation group G of order n and is one of a set of h conjugate cycles in G, then $r \cdot q \cdot h = n$.

For example, in the symmetric group on the four letters a, b, c, d, (p. 18, Exercise 3) (ab) is one of a set of 6 conjugate cycles and each appears in 2 permutations of the group. Hence, we have $r = 2$, $q = 2$, $h = 6$, $n = 24$.

Again, in the intransitive group

$$I,\ (abc),\ (acb),\ (ab)(de),\ (ac)(de),\ (bc)(de)$$

(ab), (ac), (bc) are a conjugate set, the cycles each appearing in one permutation of the group. Hence here $r = 2$, $q = 1$, $h = 3$, $n = 6$. Similarly, the theorem is illustrated with (abc) and (acb).

In proving the theorem we observe that exactly as many permutations of G transform $(a_1a_2 \cdot \cdot \cdot a_r)$ into itself as transform it into any other cycle of the set of h conjugates. Hence $\frac{n}{h}$ of the elements of G transform $(a_1a_2 \cdot \cdot \cdot a_r)$ into itself. Now the only permutations on $a_1, \cdot \cdot \cdot, a_r$ transforming $(a_1a_2 \cdot \cdot \cdot a_r)$ into itself are its own powers (§ 10, Theorem 4), r in number. Accordingly, if $(a_1a_2 \cdot \cdot \cdot a_r)$ appears in q different permutations of G, exactly $q \cdot r$ permutations of G transform $(a_1a_2 \cdot \cdot \cdot a_r)$ into itself, which gives $q \cdot r = \frac{n}{h}$.

EXERCISES

1. If in a group G the permutation A is one of a conjugate set of m permutations, prove that all the permutations of G that transform A into itself form a subgroup of index m in G. Hint. P. 26, Exercise 3, and § 15, Theorem 2.

2. Prove that the cross-cut of two groups is a group.

3. In a symmetric group of degree greater than two, show that every element except the identity has at least one conjugate distinct

from itself. Hint. In the group there is always another permutation similar to the given one and also a transforming element.

4. State and prove a theorem for alternating groups similar to that of the preceding exercise. Hint. Apply Theorem 4 of § 10 to cycles.

5. Prove that in a permutation group a conjugate set of elements (or subgroups) generates an invariant subgroup or else the group itself.

6. Prove: If a group H is invariant under exactly m elements of a group G whose order is g, then G contains a subgroup of order m, and the elements of G can be separated into g/m sets which transform H into g/m distinct conjugates, respectively.

7. Show that in a transitive group G on n letters, the permutations that leave one letter fixed form a subgroup of index n in G.

8. Employ Theorem 5 of this section to prove that the alternating group of degree four contains no subgroup of order 6.*

18. Multiple Transitivity. A permutation group on n letters which has elements replacing a given letter by each of the other letters has been defined as transitive. This definition is readily extended. A permutation group on n letters which has elements replacing k specified letters by any k of the letters is said to be **k-ply transitive** ($k \leqslant n$). Such a group evidently contains elements replacing any k letters by any k letters in the permutations of the group.

For $k = 1, 2, 3$, the group is called *simply, doubly, triply transitive,* respectively.

It is obvious that the symmetric group on n letters is n-ply transitive.

Since the alternating group of degree n contains $\begin{pmatrix} a_1a_2a_3\cdots a_n \\ a_ia_ja_r\cdots a_m \end{pmatrix}$ or else $\begin{pmatrix} a_1a_2a_3\cdots a_n \\ a_ja_ia_r\cdots a_m \end{pmatrix}$ where $i, j, r, \cdots, m$ are the integers 1, 2, $\cdots$, n in any order, evidently in the alternating group of

* Miller, G. A., *Annals of Mathematics*, vol. 25 (1924), p. 48.

degree n we can find a permutation replacing any $n-2$ letters by any $n-2$ of the n letters. Hence, the alternating group on n letters is $(n-2)$-ply transitive, but not $(n-1)$-ply transitive.

THEOREM 1. *If G is a doubly transitive group on the n letters $a_1, a_2, \cdots, a_n$, a subgroup H that leaves exactly one letter fixed is transitive on $n-1$ letters.*

Let H leave a_1 fixed. Since G is doubly transitive, the letters a_1, a_2 are replaced by elements of G by any pair of different letters. H thus contains $\begin{pmatrix} a_1 a_2 \cdots a_n \\ a_1 a_3 \cdots \cdot \end{pmatrix}$, $\begin{pmatrix} a_1 a_2 \cdots a_n \\ a_1 a_4 \cdots \cdot \end{pmatrix}$, etc., or a_2 is replaced by each of the n letters excepting a_1. Hence H is transitive and of degree $n-1$.

If the idea of this theorem is extended to a k-ply transitive group, we have:

COROLLARY. *In a k-ply transitive group of degree n a subgroup that leaves $k-1$ given letters fixed is transitive and of degree $n-k+1$.*

THEOREM 2. *The order of a k-ply transitive group G of degree n is $n(n-1)(n-2)\cdot \cdots \cdot(n-k+1)\cdot m$, where m is the order of a subgroup H that leaves k letters fixed.*

From the preceding Corollary and p. 43, Exercise 7, H is of index $n-k+1$ in a subgroup which leaves $k-1$ letters fixed; this is of index $n-k+2$ in a subgroup that leaves $k-2$ letters fixed; etc.

Again, neither H (if it is not the identity) nor any of its subgroups (excepting the identity) is invariant in G, because some element of G involving letters left fixed by H would not transform such a subgroup into itself. Hence we have

THEOREM 3. *If a k-ply transitive Group G of degree n is*

abelian and not $(k+1)$*-ply transitive, the subgroup that leaves* k *letters fixed is the identity, and the order of* G *is* $n!/(n-k)!$.

19. Primitive and Imprimitive Groups. The transitive group I, $(abc)(xyz)$, $(acb)(xzy)$, $(ax)(bz)(cy)$, $(ay)(bx)(cz)$, $(az)(by)(cx)$ bears an interesting relation to the following grouping of its six letters: $a, b, c; x, y, z$. Under each element of the group each set remains intact, or the sets are just interchanged. On this account the group is said to be imprimitive, and the two sets are called imprimitive systems. Surprisingly enough $a, x; b, y; c, z$ also are imprimitive systems for this group.

If the letters of a transitive group can be separated into equal sets which are transformed as units by each permutation of the group, the group is said to be **imprimitive** and the sets are called **imprimitive systems.** The number of the systems must be greater than one and less than the degree of the group. If no such property exists for a transitive group, it is said to be **primitive.**

Evidently no group of prime degree can be imprimitive. In other words, a transitive group of prime degree is primitive.

THEOREM 1. *If* G *is a* k*-ply transitive group and* $k > 1$, G *is primitive.*

For if $k > 1$, there would be elements in the group which would transform two letters from any given set of an imprimitive system into different sets.

THEOREM 2. *For any separation of the letters of a primitive group* G *into equal sets, there is at least one permutation of* G *that transforms two letters of any given set into two different sets.*

Without specializing the proof but to simplify the notation let there be four letters in each set: $a_1, a_2, a_3, a_4; a_5, a_6, a_7, a_8;$

a_2, etc. Suppose the contrary of the theorem; that is, that every permutation taking a_1 into the ith set, takes a_2, a_3, a_4 into the ith set, or that letters of the first set are transformed together by all permutations of G. Furthermore, since G is transitive, there would be at least four permutations of G taking the first set into each other set. It is easy to show that a_5, a_6, a_7, a_8 would likewise be transformed together by each permutation of G. For, suppose permutation S transforms the first set into the second, then the product of any permutation of G by S^{-1} (and by p. 7, Exercise 4, such products will give all the permutations of G) would transform the letters of the second set together. Etc. Accordingly, G would be imprimitive, which is contrary to hypothesis. Hence, there must be at least one permutation of G that transforms a_1 and a_2 into letters of different sets.

COROLLARY. *If the letters of a primitive group G are separated into two sets, equal or unequal, there is at least one permutation of G that transforms one letter of the first set into the second set and leaves some other letter of the first set in the first set.* (*The first set must contain more than one letter.*)

THEOREM 3. *If a primitive group G contains a transposition, G is the symmetric group.*

Suppose G is primitive on the n letters $a_1, a_2, \cdots, a_n$, and contains $A = (a_1a_2)$. If the letters are separated into the two sets a_1, a_2; $a_3, \cdots, a_n$, by the preceding Corollary G contains a permutation T which leaves one of a_1 and a_2 in the first set and transforms the other into the second set, say into a_3. Then

$$B = T^{-1}AT = (a_ia_3), \text{ where } i = 1 \text{ or else } 2.$$

Now since $(xy)(xz)(xy) = (yz)$, (a_ia_3) with (a_1a_2) would generate a third transposition, and hence the symmetric group on a_1, a_2, a_3.

If now the letters are separated into the two sets a_1, a_2, a_3; $a_4, \cdots, a_n$, we have similarly a permutation S in G which leaves one of a_1, a_2, a_3 in the first set and transforms another into the second set, say into a_4. Then

$$C = S^{-1}AS = (a_j a_4), \text{ where } j = 1 \text{ or else } 2 \text{ or else } 3.$$

Transforming C by the three transpositions already obtained gives all the transpositions of the symmetric group of degree four. These generate the symmetric group of degree four (p. 31, Ex. 7). Etc.

THEOREM 4. *A sufficient condition that a transitive group G on n (> 3) letters be imprimitive is that the subgroup H that leaves one letter fixed leaves m letters fixed where $1 < m < n$.*

Let G be transitive on the $n (n > 3)$ letters $a_1, a_2, \cdots, a_n$, and suppose the largest subgroup H_1 that leaves a_1 fixed leaves m letters $a_1, a_2, \cdots, a_m (1 < m < n)$ fixed. We take $m = 4$ in order to simplify the notation in the proof. Then H_1 leaves a_1, a_2, a_3, a_4 fixed. The subgroup consisting of all those permutations omitting a_2 must include H_1. It can be no larger, for then on transforming it by $(a_2 a_1 \cdot \cdot$ etc.) from G we should have a group containing no a_1 but larger than H_1, which is impossible. So the subgroup omitting a_2 is H_1; and similarly for a_3 and a_4. If now H_1 is transformed by $(a_5 a_1 \cdot \cdot$ etc.), a conjugate subgroup H_2 is obtained which not only omits four letters but from what has just been shown about H_1 we know that none of those four is a_1, a_2, a_3, nor a_4. Let them be a_5, a_6, a_7, a_8. Then just as for the preceding set, the subgroup omitting a_5 is H_2, a_6 is H_2, etc. If there are more letters in G, transform H_1 by $(a_9 a_1 \cdot \cdot$ etc.) and obtain H_3, which will be different from H_1 and H_2. Continuation of this process shows that m is a factor of n.

It will next be shown that these sets a_1, a_2, a_3, a_4; a_5, a_6, a_7, a_8; $a_9, a_{10}, \cdots$; $\cdots$; $\cdots a_n$ are systems of imprimitivity. We shall do this by showing that no permutation of G carries two letters, say a_1, a_2, of the first set into two different sets. Suppose permutation P carries a_1 into a_5, and a_2 into a_9; thus

$$P = \begin{pmatrix} a_1 a_2 a_3 a_4 \cdots a_n \\ a_5 a_9 \cdots \cdots \end{pmatrix}.$$

Take an element from H_2, as

$$Q = \begin{pmatrix} a_1 a_2 a_3 a_4 a_5 a_6 a_7 a_8 a_9 \cdots a_n \\ \cdots \cdots a_5 a_6 a_7 a_8 a_x \cdots \cdots \end{pmatrix}$$

in which $x \neq 9$. On forming the product PQP^{-1} we have $\begin{pmatrix} a_1 a_2 \cdots a_n \\ a_5 a_9 \cdots \cdots \end{pmatrix} \begin{pmatrix} \cdots a_5 a_6 a_7 a_8 a_9 \cdots a_n \\ \cdots a_5 a_6 a_7 a_8 a_x \cdots \cdots \end{pmatrix} \begin{pmatrix} a_5 a_9 \cdots a_x \cdots \\ a_1 a_2 \cdots a_y \cdots a_n \end{pmatrix}$, which equals $\begin{pmatrix} a_1 a_2 \cdots \\ a_1 a_y \cdots \end{pmatrix}$, where y evidently cannot equal 2 unless $x = 9$ which is contrary to hypothesis. But it is impossible for y to be different from 2 because permutations leaving a_1 fixed left a_2 fixed.

By a similar indirect method it can be shown that a_1 cannot be left in the first set and a_2 carried into another set by any permutation of G. Hence G is an imprimitive group.

EXERCISES

1. In a transitive group G of degree n, prove that, if the subgroup that leaves one letter fixed is transitive and of degree $n - 1$, G is at least doubly transitive.

2. If an abelian group is simply but not doubly transitive, show that its order equals its degree. Hint. *Cf.* § 18, Theorem 3.

3. Classify the transitive groups in the exercise list of p. 35 as to multiple transitivity.

4. If a group is at least doubly transitive and contains a transposition, prove that it is the symmetric group. Hint. See p. 31, Exercise 7.

5. Prove: The number of systems of imprimitivity is a factor of the degree of the group involved. Indicate which groups in the exercise list of p. 35 are imprimitive.

6. Prove: (*a*) The degree of an imprimitive group is composite; (*b*) a transitive group whose degree is prime is primitive.

7. Show that a regular cyclic group of composite order is imprimitive.

8. In a primitive group G, if the subgroup that leaves one letter fixed is transitive, prove that G is at least doubly transitive.

20. Isomorphisms. On pages 23, 28–29, 30 a one-to-one correspondence of the elements of one group with those of another was used. It is the purpose of the present section to make further study of relations between two groups. Naturally the simplest comparison would be between two groups of the same order. Suppose that the group of § 2, $G = [I, P, Q, R, A, B]$,* which was the group of rotations of three concurrent half lines of a plane each making an angle of 120° with the others, be taken as one group. In this $P^2 = I$, $Q^2 = I$, $R^2 = I$, $A^3 = I$, $B^3 = I$; some elements are of period 2, some of period 3.

If the symmetric group on the three letters a, b, c (*Cf.* § 8), $G' = [I, (abc), (acb), (bc), (ac), (ab)]$, is compared with G, it is seen that each contains besides the identity, two elements of period 3 and three of period 2. Let the groups be paired off, paired elements to be of the same period. In setting up the correspondence, to A must correspond an element of period 3, either (abc) or (acb); take (abc). Then to B naturally corresponds (acb), and this so much the more because $B = A^2$ and $(acb) = (abc)(abc)$. Now to P, Q, R must correspond (bc), (ac), and (ab), in some order. Take (bc) to correspond to P. Now in

I	I
A	(abc)
B	(acb)
P	(bc)
Q	(ac)
R	(ab)

* Brackets are frequently used to inclose the elements of a group.

G, $A \cdot P = Q$; hence, corresponding to Q is placed the product $(abc) \cdot (bc)$ which is (ac). Similarly, $B \cdot P = R$; so that $(acb) \cdot (bc)$, or (ab), is made to correspond to R. It might be verified for a few other products that to the product (in a chosen order) of any two elements in G corresponds the product (in the same order) of the two corresponding elements of G'. One-to-one correspondence possessing this product property throughout the set is known as **simple isomorphism, or 1:1-isomorphism.** As far as abstract properties are concerned, such as subgroups of various kinds, elements with particular abstract properties (*e.g.*, invariance) evidently two simply isomorphic groups are identical. Hence, whatever abstract properties are discovered in one of the groups are properties of the other. Will transforms involving corresponding elements themselves correspond?

I	I
B	(abc)
A	(acb)
R	(ac)
Q	(ab)
P	(bc)

We observe that with the groups used in this illustration the isomorphism can be set up in other ways, and this is generally true of groups that can be paired in simple isomorphism at all. Another simple isomorphism of these groups is given at the left.

The law stated for isomorphic correspondence restricts the number of different pairings possible. Thus, the 1:1-correspondence at the right is not isomorphic; because while in G, $A \cdot P = Q$, in G', $(abc) \cdot (bc) \neq (ab)$. Since a cyclic group is abelian, evidently to the various powers of any element of one of two groups in simple isomorphism must correspond the same powers, respectively, of an element (of the same period) in the second group.

I	I
A	(abc)
B	(acb)
P	(bc)
Q	(ab)
R	(ac)

General isomorphism is illustrated at the right of this para-

graph. Each group is separated into the same number of sets of elements, two sets here. In each group: the upper set is an invariant subgroup; the even powers of elements in the lower set are in the upper set, odd powers in the lower set itself; the product of an element of the upper set by one of the lower set is in the lower set; etc. A **general isomorphism** thus differs from the simple isomorphism in that the elements of each group are separated into sets, and instead of a correspondence between pairs of elements it is between pairs of sets, in which lie corresponding elements and products. The general isomorphism in the illustration may be called a 3:2-isomorphism.

I	I
(abc)	$(ac)(bd)$
(acb)	
(ac)	$(abcd)$
(ab)	$(adcb)$
(bc)	

Evidently all the products and powers (made up of n factors) of the elements in any given set must be in some one set of the group. From this fact it is seen that the set containing I must be a subgroup. Moreover, this subgroup H is invariant in its group G, because, since the transform of I is in H, the transform of each element of H by elements of G must be in H. Finally, if H contains h elements, each set contains exactly h elements. To prove this, let $H = [I, A, B, \cdots, F]$ and let L be an element in some other set. Since $L \cdot I$ is in this set, LA, LB, $\cdots$, LF are in the set, and it has at least h elements. Suppose the set contains K besides. Now $K = LX$ (p. 7, Ex. 4) where from the immediate assumptions X is not in H. If the period of L is m, then $L^{m-1} \cdot LA$ is in H; and if K is in the set, the product $L^{m-1}K$ must likewise be in H. Since $K = LX$, the contrary results, because $L^{m-1}K = L^{m-1}LX = X$, which is not in H. Hence, each of the sets contains exactly h elements, and furthermore, *in a general isomorphism G is seen to be separated into co-sets as regards an invariant subgroup H.*

EXERCISES

1. Prove: If two groups are in simple isomorphism, transforms (or commutators) involving corresponding elements correspond.

2. Set up a simple isomorphism between the group in § 1 and group (6) in the exercise list of p. 35.

3. Set up a general isomorphism between the octic group and the symmetric group on three letters.

4. Find all the ways that a cyclic group of order five can be made simply isomorphic with itself. Suggestion. Use the substitution $(abcde)$ to generate the group.

21. Construction of Intransitive Groups. A little study of the group,

$$I, \quad (abc), \quad (acb), \quad (de), \quad (abc)(de), \quad (acb)(de)$$

reveals that it is made from the groups I, (abc), (acb) and I, (de) by multiplying the elements of one by the elements of the other. The two groups are on different sets of letters, so that this multiplication is easily effected and the period of each product is known to be the lowest common multiple of the periods of the factors. (*Cf.* p. 15, Ex. 8.) Any group thus formed is intransitive and its order is the product of the orders of the groups used as factors and its degree the sum of their degrees. More than two groups may be similarly multiplied together. Thus, from

$$I, (abc), (acb); \quad I, (def), (dfe); \quad I, (ghi), (gih)$$

we should obtain an intransitive group of order 27 and degree 9. Since each of the factors is abelian, the resulting product is abelian. We observe that the product is abelian if and only if all of the factors are abelian.

This method for constructing intransitive groups is called the **direct product method.** Another way is the **isomorphism method.** Bolza has shown that all methods are based upon these two.* We shall next build up some groups by the second

* O. Bolza, *American Journal of Mathematics*, vol. 11 (1889), p. 195.

method, using transitive constituent groups, since it can be demonstrated that an intransitive group is composed of transitive constituents.

Take two symmetric groups of degree 3, one on a, b, c, and one on d, e, f, and set up a simple isomorphism, as shown. The new group is formed by multiplying corresponding elements; thus, giving

I	I
(abc)	(def)
(acb)	(dfe)
(ab)	(ef)
(ac)	(de)
(bc)	(df)

$$I,\quad (abc)(def),\quad (acb)(dfe),$$
$$(ab)(ef),\quad (ac)(de),\quad (bc)(df).$$

Each element of the resulting group consists of two parts which have the same abstract properties. In fact, the resulting group here is abstractly identical with either of the constituents, but as a permutation group it is different, for it is intransitive and of degree 6, while each of them is transitive and of degree 3.

From the illustration at the right evidently the number of constituents is unlimited, and we see that any given group of finite order can be represented in numberless ways.

I	I	I
(abc)	(def)	(gih)
(acb)	(dfe)	(ghi)

In the section on isomorphisms (§ 20) we saw that if the co-set of the elements of the group G containing the identity is an invariant subgroup (H), the other co-sets behave as units under all elements of the group; that is, if by some operation element A (of G) took one element of the ith co-set over into the jth co-set, it took every element of the ith co-set into the jth co-set. Furthermore, these co-sets possess the necessary qualifications of a group. For, one element of a co-set effects the same interchange among the co-sets as does any other element of that set. The co-sets thus act as units, and the

number of the units in this set equals the index of the invariant subgroup H. This set of units is closed, for the product of an element from one unit by an element from another is in the set. The invariant subgroup H plays the rôle of the identity, and the set is finite. The co-sets thus behave as elements of a group whose order equals the index of H and whose elements have the same abstract relations among themselves as have the corresponding co-sets (of G) among themselves. This group is called the **quotient group** (Q) of G with respect to H. G/H is frequently used to represent this quotient group Q.

I	I	I	I	I	I
$(km)(ln)$		$(ab)(cd)$		(xyz) (xzy)	
$(klmn)$	(ef)	$(ac)(bd)$	(ef)	(xy) (xz)	(ef)
$(knml)$		$(ad)(bc)$		(yz)	

In each of the three illustrations preceding this paragraph the co-set corresponding to (ef) acts (as an aggregation) in its group just as (ef) does in its group. If now in each illustration corresponding parts are multiplied, evidently the resulting elements are made up of factors that behave alike, and the product is an intransitive group. For example, from the first we have the following intransitive group of order four and degree six:

$$I, \quad (km)(ln), \quad (klmn)(ef), \quad (knml)(ef).$$

I	I
$(ab)(cd)$	(xyz) (xzy)
$(ac)(bd)$	(xy)
$(ad)(bc)$	(xz) (yz)

Or again, since the quotient groups in the second and third multiple isomorphisms above are abstractly identical, we can set up the 2:3-isomorphism shown here at the left. On multiplying the elements of corresponding co-sets here, an intransitive group of order 12 and degree 7 is obtained.

From what has just been developed we have the following theorem indicating when two groups on different letters can be used as isomorphic constituents:

THEOREM. *Two groups G and G' can be placed in general isomorphism, if and only if G contains an invariant subgroup H and G' an invariant subgroup H', such that the quotient groups G/H and G'/H' are simply isomorphic. One or both H's may be the identity.*

EXERCISES

1. Write the intransitive group of order 12 and degree 7 resulting from the general isomorphism in this section.

2. By the direct product method obtain three different intransitive groups of order 16.

3. Write the intransitive group resulting from the general isomorphism set up between the octic group and the symmetric group on three letters. See p. 52, Ex. 3.

4. The symmetric group G on four letters contains a four-group H as an invariant subgroup. Find the quotient group G/H.

5. Assuming that every intransitive group is constructible from transitive constituent groups, prove: *The average number of letters in the permutations of an intransitive group of degree n is at most $n - 2$.* Hint. Apply Frobenius' theorem (§ 14, Th. 3) to the transitive constituents.

22. Invariant Subgroups of Symmetric and Alternating Groups.

If a group as I, (abc), (acb) has no invariant subgroup besides the identity, it is said to be a **simple group.** One that has an invariant subgroup (other than I) is said to be **composite.**

LEMMA 1. *Any positive permutation equals the product of cycles of degree three.*

Such a permutation factors into an even number of transpositions. That every pair of contiguous transpositions can be

replaced by one or more cycles of degree three is shown by the following identities:

(*a*) If the transpositions have no letter in common,
$(ac)(bd) \equiv (abc)(bcd)$.

(*b*) If the transpositions have one letter in common,
$(ac)(bc) \equiv (abc)$.

(*c*) If the transpositions have both letters in common,
$(ac)(ac) \equiv I$.

LEMMA 2. *The group G produced (or generated) by using as permutations every cycle of degree three on n letters, $n > 2$, is the alternating group of degree n.*

Evidently G is positive. Each positive permutation on the n letters is equal to the product of an even number of transpositions (§ 10). From the preceding Lemma pairs of the contiguous transpositions could be replaced by cycles of degree three on the same letters. Hence, these cycles of degree three generate all the positive permutations on the n letters and no other permutations. These positive permutations compose the alternating group of degree n (§ 12).

THEOREM 1. *The alternating group of degree n, $n \neq 4$, is simple.*

If $n = 2$ or 3, this is obvious; and when $n = 4$, the four-group is an invariant subgroup. Hence we proceed to prove the theorem for $n > 4$, and we do this by showing that any supposed invariant subgroup contains all the possible circular permutations of degree three on the n letters, and by Lemma 2 is, accordingly, the alternating group itself.

Let the alternating group G be on the $n(n > 4)$ letters, a, b, c, d, e, etc., and suppose that A is an element of lowest degree in the supposed invariant subgroup H.

First. A can contain no cycle of more than three letters, for if

$$A = (abcd\cdots)(\cdots),$$

then the transform by

$$B = (abc) \text{ from } G, \text{ which is}$$

$$B^{-1}AB = (bcad\cdots)(\cdots)$$

would be in H (since H is invariant in G); and

$$A^{-1}B^{-1}AB = (\cdots dcba)(\cdots)\cdot(bcad\cdots)(\cdots)$$
$$= (c)(bda\cdots),$$

which would be in H and contain fewer letters than does A. But this is contrary to the supposition. Hence, no element of H contains a cycle of more than three letters.

Second. If A has a three-letter cycle, it has no other letters; for if

$$A = (dab)(c\cdots),$$

then

$$B^{-1}AB = (dbc)(a\cdots) \text{ is in } H, \text{ and so is}$$

$$AB^{-1}AB = (dab)(c\cdots)(dbc)(a\cdots)$$
$$= (b)(ac\cdots),$$

which is of lower degree than is A. But this is impossible, because H contains no element of lower degree than A is. Hence, if A contains a three-letter cycle, it contains no other letters.

Third. A cannot be made up of a single transposition, for G contains no negative permutations.

Fourth. A cannot be made up of two or more transpositions, for if

$$A = (ab)(de)(\cdot\cdot)(\cdot\cdot),$$

then

$$B^{-1}AB = (bc)(de)(\cdot\cdot)(\cdot\cdot),$$

and

$$AB^{-1}AB = (ab)(de)(bc)(de)(\cdot\cdot)(\cdot\cdot)$$
$$= (d)(e)(ac)(\cdot\cdot)(\cdot\cdot\cdot),$$

which is impossible for this would be of lower degree than A is. (Note that if $n = 4$, we could not use a, b, c, d, e). Hence A cannot be made up of two or more transpositions.

Conclusions. From these four steps it is evident that A is of type (abc). Since an alternating group of degree > 4 is at least triply transitive (§ 18), G contains elements that transform A into every three-letter permutation possible on the n letters, and all these are in H (because H is assumed invariant). Then by Lemma 2, H coincides with G, and G is simple.

Theorem 2. *The only invariant subgroup (besides the identity) contained in the symmetric group of degree n, $n \neq 4$, is the alternating group of degree n.*

The preceding proof can be used excepting the reason in the third step for excluding a transposition. In the proof of the present theorem, A cannot be a simple transposition, for then H would contain every transposition on the n letters (§ 18), and accordingly H would be the symmetric group itself (p. 48, Ex. 4).

23. Groups of Degrees Two, Three, and Four. The permutation groups of degree less than twelve have been worked out and published. Cayley's notation is frequently used to represent groups in such lists. We have developed theory and technique sufficient to enable us to study the groups of degrees two, three, and four. It will be helpful to recall that the degree of a transitive group is a factor of its order (§ 14, Th. 2); that, since an intransitive group is composed of transitive constituents, an intransitive system must contain at least two letters; that every group of degree n is a subgroup in the symmetric group on those n letters, hence its order is a divisor of $n!$.

Degree Two. Obviously the only group on a, b is $[I, (ab)]$.

Degree Three. All groups of degree three besides the symmetric group $[I, (abc), (acb), (ab), (ac), (bc)]$ are sub-

groups of it, and hence the possible orders are 2 and 3. But the subgroups of order two are not of degree three. The alternating group $[I, (abc), (acb)]$ is the only one of order three.*

Degree Four. Intransitive Groups. For an intransitive group there must be at least two transitive constituents and each must involve at least two letters; hence, this (i.e., four) is the lowest degree for which there are intransitive groups. Using (ab) and (cd), we have as a direct product the four-group $[I, (ab), (cd), (ab)(cd)]$, while the isomorphism method gives a group of order two, $[I, (ab)(cd)]$. (See § 21.)

Transitive Groups. From the observations at the beginning of this section the possible orders for transitive groups of degree four are four, eight, twelve, and twenty-four.

There can be no group of order twenty-four on four letters other than the symmetric group of degree four consisting of all the permutations on the four letters. Using a, b, c, d we have

$I,$	$(abc),$	$(acb),$	$(abcd),$	$(ab),$
$(ab)(cd),$	$(abd),$	$(adb),$	$(abdc),$	$(ac),$
$(ac)(bd),$	$(acd),$	$(adc),$	$(acdb),$	$(ad),$
$(ad)(bc),$	$(bcd),$	$(bdc),$	$(acbd),$	$(bc),$
			$(adbc),$	$(bd),$
			$(adcb),$	$(cd).$

In transitive groups of order four the permutations (other than the identity) must each be of degree four (p. 36, Ex. 7). These are of type $(abcd)$ or $(ab)(cd)$. The former gives the cyclic group $[I, (abcd), (ac)(bd), (adcb)]$, and the latter gives

* We should remark here that if one permutation group can be transformed by some permutation into another permutation group, the two groups are not considered as different permutation groups; thus, $[I, (ab)]$, $[I, (bc)]$, $[I, (xy)]$ as permutation groups are identical.

rise to the four-group $[I, (ab)(cd), (ac)(bd), (ad)(bc)]$. (*Cf.* § 13.)

If there is here a group of order eight, its permutations (besides the identity) can be only of period two or four (§ 11, Th. 1, Cor. 1). It must contain at least three permutations of degree four (p. 36, Ex. 7); and it must be generated by its permutations of degree four (p. 36, Ex. 10). Why? It must contain a permutation of period four; for, otherwise, it would be a commutative group (p. 27, Ex. 10) and contain a four-group. But neither of the four-groups found has permutations each commutative with any outside permutation of period two in the symmetric group of degree four. Hence, $H \equiv [I, (abcd), (ac)(bd), (adcb)]$ is a subgroup of every possible group of order eight and degree four, and it is invariant (§ 11, Th. 2). There must be another permutation of degree four in it, for its permutations of degree four must generate it. Finally, since $(ac)(bd)$ must be invariant under this permutation of degree four, it cannot be one of those of period four. Hence the group, if such there be, must be obtained by extending H by $(ab)(cd)$. This gives the octic group (§ 14), and the reasoning shows that it is the only group of degree four and order eight.

We know that there is one group of order twelve, which is the alternating group consisting of all the positive permutations on four letters. If there is any other group of order twelve here, it must, accordingly, contain both positive and negative permutations, and its positive permutations must form a subgroup of order six (§ 12, Th. 1). Since we have found no such group of order six on three or four letters, there is no other group of order twelve and degree four.

EXERCISES

1. Show whether the following would be equivalent to the definition in § 13: A permutation group on the h letters $a, b, c, \cdots, n$ is transitive if the elements replace letter a by each of the other letters.

2. If H is an invariant subgroup of a transitive group G of degree n, H is of degree n or is the identity.

3. If a group of degree n has as elements the transposition (a_1a_2) and the circular permutation $(a_1a_2a_3\cdots a_n)$, it is the symmetric group of degree n.

4. If two transitive groups of degree n have in common their elements of degree n, then they differ only in elements of degree $n-1$. Hint. P. 36, Ex. 9.

5. In an imprimitive group, G, all the elements that permute the letters within their systems but do not interchange any systems, form an invariant intransitive subgroup of G.

ADDITIONAL EXERCISES

1. If S is a permutation of m cycles of degrees $c_1, c_2, \cdots, c_m$, respectively, no two cycles having a common letter and no two of the same degree, then all the permutations on exactly the same letters, which are commutative with S, form a group G which is the direct product of cyclic groups generated by the individual cycles. (§ 10, Th. 4.) G is thus of order $c_1 \cdot c_2 \cdots c_m$ and abelian; it will be cyclic if no two c's have a common factor greater than 1.

2. Represent the groups of § 23 in Cayley's notation. *Cf.* Quarterly Journal of Mathematics, vol. 25 (1890–91), pp. 71, 137.

3. Discuss the possible groups of degree five. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), p. 45.

4. If H and K are two subgroups of a group G, and H is invariant, then the cross-cut L of H and K is invariant in K. If both H and K are invariant in G, L is invariant in G. Cole's Netto, *Theory of Substitutions* (1892), § 71.

5. Write a paper showing that if an intransitive group G is composed of two transitive constituents, it is formed from them either by the direct product method or else by the isomorphism method. See Burnside, *Theory of Groups* (1897), § 114–116 or (1911), §§ 142–144 and Hilton, *Finite Groups* (1908), p. 92.

6. Use Theorem 5 of § 17 to discuss the groups of degree four. *Cf.* Miller, G. A., *Annals of Mathematics*, vol. 25 (1924), p. 49.

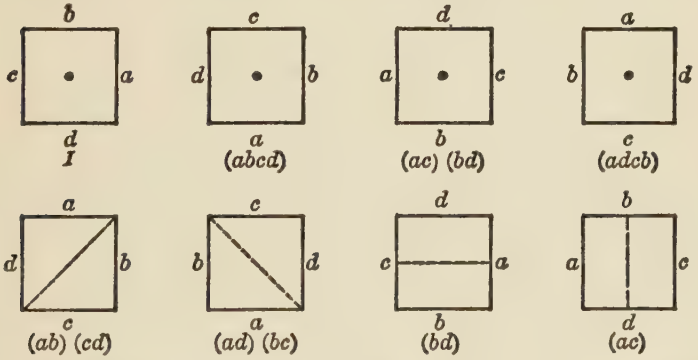
CHAPTER IV

SOME GROUPS OF MOVEMENTS AND OTHER SPECIAL GROUPS

24. Introduction. In Chapter I two or three groups of movements were used in introducing the idea of groups. We can now take up a little more detailed study of some special groups, because we have more group theory at our command. By a movement of a rigid body we shall understand an operation which carries the body from one position into another position. Since the body is rigid and remains intact, the distance between any two of its points remains unaltered; and, furthermore, the angle between any two of its lines remains unaltered. Accordingly, these distances and angles are invariant under the movements. In each movement it is the body's new position relative to its original position that is important rather than the intermediate condition or the path or the moving itself.

The law of combination of two movements simply means that if A represents one movement of the body and B (which may be the same or different from A) represents a movement of the body, then AB means a single movement equivalent to movement A followed by movement B, carrying the body from its position just before movement A directly to the final position in which it was left by B. Accordingly, the product of any two or more movements of the body is equivalent to a single movement. The associative law holds, and the identity may be thought of as the rotation of the body about an axis through $n \cdot 360°$ (where n is an integer). Reversing movement A gives the inverse, A^{-1}, of the movement A.

25. Group of the Square. Let us study the group of movements of a square whose sides in succession are a, b, c, d, the movements being such that the vertices always fall in the four original positions. Besides the identity, I, there are: first, rotations in the plane of the square about its center, through 90°, 180°, 270°. A rotation through 90° replaces side a by side b, b by c, c by d, and d by a, all of which is compactly denoted by the permutation $(abcd)$. Repeating this rotation, which symbolically would be $(abcd) \cdot (abcd)$ or $(ac)(bd)$, gives rotation through 180°; and similarly, $(abcd)^3$ or $(adcb)$ gives rotation through 270°; and $(abcd)^4$ gives rotation through 360°. (Note that $(abcd)^4 = I$.)

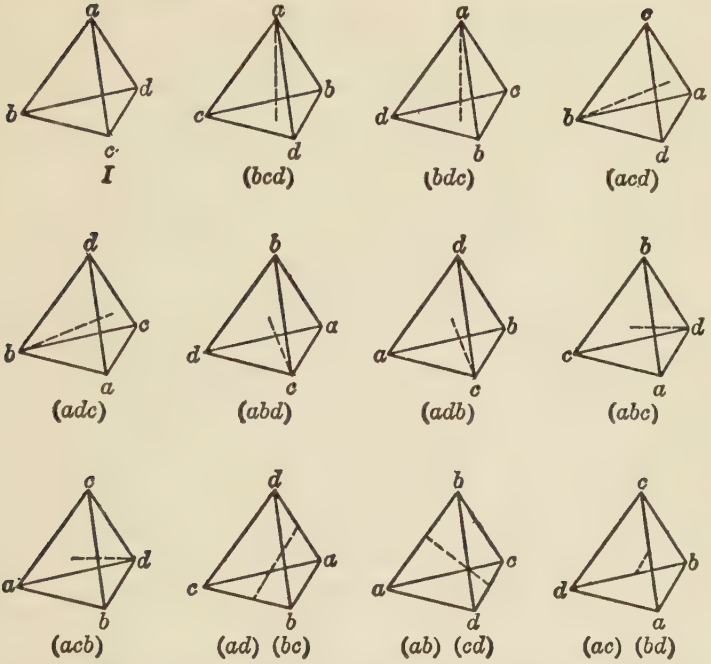


Besides rotation in its plane around its center (with respect to which the square is symmetric), the square can be turned or rotated around its four lines of symmetry (which are the diagonals and the lines joining the mid-points of each pair of opposite sides). From the figure we see that these movements give rise to $(ab)(cd)$ and $(ad)(bc)$, and similarly rotations about the other two axes of symmetry give (bd) and (ac). Since there are no movements other than these eight taking the square into

itself as a rigid body, they form a closed set. The student with curiosity will want to combine two of these movements that are of different types. Take, for example, the movements represented by $(ab)(cd)$ and $(abcd)$ and show that the result agrees with the product $(ab)(cd) \cdot (abcd)$. This group of movements of the square is but one of an infinite number of groups called **dihedral groups**, which correspond to groups of movements of regular polygons.

26. Group of the Regular Tetrahedron. It is interesting to obtain the group of movements into itself of a solid, as of the regular tetrahedron. In working this out as a permutation group we may use a letter on each edge, six in all; or one on each face, four in all; or one for each vertex, four in all. Let us employ the last mentioned method and use a, b, c, d, as shown in the following figures. Evidently every axis of rotation must be perpendicular to every face of the tetrahedron that it meets and must meet such a face at its center so that the face will be carried into itself by rotations of the tetrahedron about the axis. Similarly, if an axis meets an edge of the tetrahedron, it must be a perpendicular bisector of that edge. Finally, an axis may pass through a vertex. Now, of the first kind, we know there are four axes, one for each face, and that each extends through the opposite vertex. Of the next kind there are three, each passing through the center and perpendicular to two edges at their mid-points. As these constitute all the possible axes, rotations of the tetrahedron into itself about them constitute a closed set.

After the identity, suppose we consider rotation through 120° about an axis through vertex a giving the permutation (bcd). Rotation through another 120° gives $(bcd)^2$ or (bdc).



Similar rotations about axes through b, c, d give more permutations of degree three. Rotation through 180° about the axis joining the midpoints of edges ad and bc gives the permutation $(ad)(bc)$. Similarly, we obtain $(ab)(cd)$ and $(ac)(bd)$. The group is of order 12 (*cf.* p. 31, Ex. 1) and the twelve positions are shown in the accompanying figures. With each figure is given the permutation which represents what change has been made from the original position to obtain the particular position. Verify by the rotations that $(bdc) \cdot (ad)(bc) = (adb)$.

27. A Group of Line Movements and a Group of Paths.

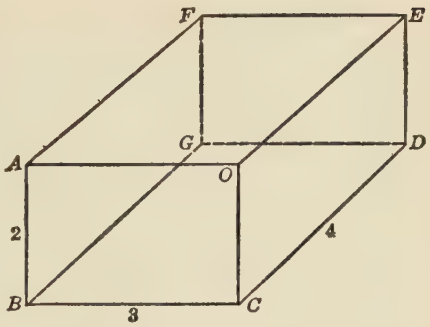
A Group of the Straight Line. The following group dif-

fers from the preceding ones in not being of finite order. Consider a straight line extending infinitely east and west. Let us find the group of movements which carry the straight line into itself. First, there are movements which consist in sliding the line along itself eastward or westward through any distance. Let A be the translation through a units eastward, say. The inverse, A^{-1}, is obviously translation a units westward. Then A^2 will be translation through $2a$ units; etc. These translations, including $A^0 = I$, form a group containing an infinite number of translations. But this is not the entire group we seek. If the line is turned end-for-end about some one of its points, say π, we have a rotation Π. Evidently $\Pi^2 = I$. Since the point π can be any point of the line, an infinite number of rotations is possible. Together with the translations just mentioned (where a takes all real values, rational and irrational) they form the required group. The given straight line is invariant under the group.

It is interesting to note that the product $\Pi\Delta$ of two rotations Π and Δ whose fixed points are π and δ, respectively, l units apart, will be a translation through $\pm 2l$ units. Does the product of two translations equal a translation? To what is the product of a translation and a rotation equal? Any two translations are commutative. Are a translation and a rotation commutative? Is a rotation about one point commutative with a rotation about a different point?

A Group of Routes. Suppose the elements of a group are made up of routes along the edges (from corner to corner) of a rectangular box whose base is 3 by 4 and whose height is 2. From each corner runs one and only one edge of each of the lengths 2, 3, 4. A route is the path along any one or more

joining edges of the total twelve; and, starting at any corner, the period of a route is the number of times that route must be repeated to return to the given corner. If we employ "2, 3" to indicate the route along an edge of length 2, thence along a connecting edge of length 3, we have (see accompanying figure) the following tables:



Route	Period	Products	The Group
2	two	0 is evidently the identity	0
3	two	2, 2 = 3, 3 = 4, 4 = 0	2
4	two	2, 4, 4, 3 = 2, 3	3
2, 3	two	2, 3 = 3, 2	4
4, 2	two	2, 4 = 4, 2; etc.	2, 3
2, 3, 4	two	2, 4, 3, 4 = 2, 4, 4, 3 = 2, 3; etc.	3, 4
3, 2, 4	two	2, 3, 4 = 3, 4, 2 = 4, 2, 3 = 2, 4, 3	4, 2
Etc.		Etc.	2, 3, 4

If one corner is selected as the initial one (see figure), the elements of the group are seen to be the routes to the eight corners. Abstractly, the group is abelian, of order eight, and consists of an identity and seven elements of period two.

EXERCISES

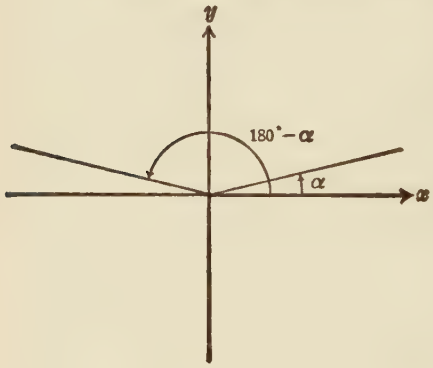
1. Obtain the group of movements of a rectangle (not a square) into itself.

2. Obtain the group of rotations of the six-spoke wheel in § 1 as a permutation group.

3. Find the group of movements of an equilateral triangle into itself.

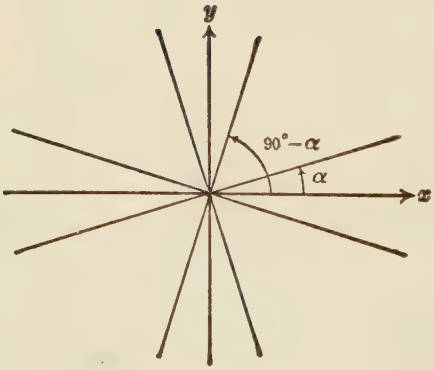
4. Study the group of movements of a regular n-sided polygon into itself. What is the order of this (dihedral) group? What is the subgroup given by rotations about an axis through its center and perpendicular to its plane? What is the period of each of the permutations outside this subgroup? How does each of these outside elements transform each element of the subgroup mentioned? Hint. Use $a_1, a_2, \cdots, a_n$ for the vertices.

5. Find the group of movements of a cube into itself. Suggestion. Use a letter for each face. What other letterings could be employed?



6. In the group of the straight line (§ 27), what is the period of the product of rotations about two distinct points? About three distinct points? Generalize.

7. Inscribed in a circle is a hexagon whose sides in order are 1, 2, 1, 2, 1, 2. The three long diagonals of length 3 are drawn. Discuss the group of routes along the straight lines connecting the six vertices.



28. Group of Certain Operations on a Given Angle. If we take any angle α and consider the operation of finding the supplementary angle, we

have two angles, α and $180° - \alpha$. Should we introduce the operation of finding the complementary angle, we should have exactly eight angles: α, $90° - \alpha$, $90° + \alpha$, $180° - \alpha$, $180° + \alpha$, $270° - \alpha$, $270° + \alpha$, $360° - \alpha$. The eight operations corresponding to these eight angles are easily seen to form a group of order eight. Use the adjacent figures (p. 68) in verifying some "products" of operations on various angles of the set. (Note. $\alpha \neq n \cdot 90°$.)

29. Group Generated by an Imaginary *n*th Root of Unity. From the theory of equations we know that the equation $x^n = 1$, or $(x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1) = 0$, $n > 2$, has the real root 1 and $n - 1$ distinct complex roots (including -1 if n is even). The roots are representable by

$$\cos \frac{360° \cdot k}{n} + i \sin \frac{360° \cdot k}{n}$$

where $i = \sqrt{-1}$, and $k = 0, 1, 2, \cdots, n - 1$. That each of these complex numbers satisfies $x^n = 1$ is easily proved by using DeMoivre's theorem

$$(\cos \theta + i \sin \theta)^n = \cos n\theta + i \sin n\theta.$$

If the law of combination is multiplication, it is seen that these n complex numbers give rise to a group of order n. By DeMoivre's theorem the successive integral powers of

$$\cos \frac{360°}{n} + i \sin \frac{360°}{n}$$

are seen to be these n roots. Hence, the group is a cyclic group of order n.

30. Certain Congruence Groups. In the present section we make a brief study of a representation which facilitates the analysis of certain groups. To this end we note that for the

integers a, b, and m, $a \equiv b \pmod{m}$, (read "a is congruent to b modulo m") means that m is a factor of the difference between a and b. If all positive integers are divided in turn by m, the remainders will be $0, 1, 2, \cdots, m-1$; that is, any integer positive or negative is congruent, modulo m, to some one of this set of m integers, which is called a **complete residue system, modulo m.** Note that there are other equivalent complete residue systems, modulo m; as, $0, 2, 3, \cdots, m-1, m+1$. If from the integers of a complete residue system, modulo m, those are chosen that are mutually prime to m, we have a **reduced residue system, modulo m.** (1 is included in this set.) Thus we have: complete residue system, 1, 2, 3, 4, 5, 6, 7, 8, 9, (mod 9); reduced residue system, 1, 2, 4, 5, 7, 8, (mod 9).

Example One. Under addition a complete residue system, (mod m), forms a cyclic group of order m. For the elements are $0, 1, 2, 3, \cdots, m-1$ and the set is closed; 0 is the identical element; the inverse of v is evidently $m - v$(or $-v$); the associative law holds.

Example Two. Under multiplication a reduced residue system (mod m), forms an abelian group. For if each of two integers is prime to m, evidently their product is likewise, so that the set is closed; 1 is the identical element; the order of multiplication is immaterial; the associative law holds. To show that any integer of the set, as v, has an inverse, multiply each integer of the reduced residue system by v. The resulting products are distinct and can easily be seen to form a reduced residue system (mod m); hence, some product is congruent to 1, and v has an inverse.

Example Three. As another group involving congruences we shall consider all the linear substitutions arising from

$$x' \equiv x + a \pmod{m}. \quad (a \text{ is an integer.})$$

These are seen to be $x' \equiv x+0$, $x' \equiv x+1$, $x' \equiv x+2$, $x' \equiv x+3$, $\cdots$, $x' \equiv x+m-1$, (mod m). Hence the group is of order m. Its identity is $x' \equiv x \pmod{m}$. Substituting $x' \equiv x+1$ into itself gives $x'' \equiv (x+1)+1$, or $x' \equiv x+2$; substituting again gives $x'' \equiv (x+1)+2$; etc. We see from this that the substitution $x' \equiv x+1$ will generate the group, and the group, accordingly, is cyclic.

31. Quaternion Units and Matrices as Elements.

Example One. The four quaternion units $1, i, j, k$ generate, when combined by multiplication, a group of order eight called the *quaternion group*. The products are defined by the equations,

$$\begin{aligned} i^2 = \quad j^2 = k^2 &= -1, \\ ij &= -ji = k, \\ jk &= -kj = i, \\ ki &= -ik = j.* \end{aligned}$$

The group is thus: $1, -1, i, -i, j, -j, k, -k$, consisting of one element of period two and six of period four, besides the identity.

Example Two. We close this Chapter with two groups of small order whose elements are square matrices. The law of combination is multiplication.†

Successive integral powers of the matrix $\begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}$ give exactly four matrices:

$$\begin{Vmatrix} 0 & 1 \\ -1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} 0 & -1 \\ 1 & 0 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}.$$

* *Cf.* Fine, H. B., *Number-System of Algebra* (1907), §127.

† See Bocher, M., *Higher Algebra* (1907), § 22 for definition of product of two nth order matrices.

The last of these is the identity. While the foregoing constitute the cyclic group of order four, the following make up the four-group:

$$\begin{Vmatrix} -1 & 0 \\ 0 & 1 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} -1 & 0 \\ 0 & -1 \end{Vmatrix}, \quad \begin{Vmatrix} 1 & 0 \\ 0 & 1 \end{Vmatrix}.$$

EXERCISES

1. Show that the group in § 28 is abstractly the octic group. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), pp. 6, 7.

2. In plane analytics the symmetry of a curve with respect to the x-axis is indicated by invariance of the xy-equation when x is replaced by x and y by $-y$; similarly, symmetry in the y-axis by invariance under $\begin{pmatrix} x & y \\ -x & y \end{pmatrix}$. In this connection study the group generated by $\begin{pmatrix} x & y \\ x & -y \end{pmatrix}$ and $\begin{pmatrix} x & y \\ -x & y \end{pmatrix}$. For the analogous theory in solid analytic geometry, what is the group and what is the meaning (about symmetry) of each of its elements?

3. In connection with the group of § 29 plot in the complex plane the n nth roots of unity and compare the results of multiplications with the rotations of an n-spoke wheel. *Cf.* § 1; p. 7, Ex. 3; p. 68, Ex. 4. What relation is there between these two groups?

4. Show that the roots in § 29 form a closed set under multiplication. The following property of complex numbers may be used here: $(\cos\theta_1 + i \sin\theta_1)(\cos\theta_2 + i \sin\theta_2) = \cos(\theta_1 + \theta_2) + i \sin(\theta_1 + \theta_2)$.

5. (*a*) Show that under addition 0, 1, 2, 3, 4, 5, 6, 7 (mod 8), is a cyclic group of order 8.

(*b*) Show why the group in Example One of § 30 is cyclic.

6. Follow the suggestion in Example Two of § 30 and thereby show that each number in the reduced residue system 1, 2, 4, 5, 7, 8 (mod 9), has an inverse under multiplication.

7. Show that under multiplication the reduced residue system 1, 3, 5, 7 (mod 8), forms an abelian group. Is it cyclic?

8. Show that under multiplication the reduced residue system 1, 2, 3, 4, 5, 6 (mod 7), forms an abelian group. Is it cyclic?

9. Study the group of the substitution $x' \equiv ax \pmod{p}$, where p is a prime and a has the values $1, 2, 3, \cdots, p-1$.

10. The successive powers of the matrix $\begin{Vmatrix} 1 & -1 \\ 1 & 0 \end{Vmatrix}$ form a group. Write down all the elements of the group.

ADDITIONAL EXERCISES

1. *Cross-ratio Group.* Show that the following substitutions form a group: $x' = x$, $x' = \frac{1}{x}$, $x' = 1 - x$, $x' = \frac{1}{1-x}$, $x' = \frac{x}{x-1}$, $x' = \frac{x-1}{x}$.

(Note. The method for combining is the substitution of one element into another.)

2. The groups of all the regular polyhedrons have been thoroughly studied. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), §§ 57, 58; or Dickson, *Modern Algebraic Theories* (1926), Chapter XIII. Work out the group of the regular octahedron.

3. Find out what values (forms) m may have in order that under multiplication the reduced residue system, modulo m, shall be a cyclic group. *Cf.* Mathews, *Theory of Numbers* (1892) §§ 19–29; or Dickson, *Introduction to the Theory of Numbers* (1929), § 17.

4. For a matrix that will generate a cyclic group of order m, where m is any positive integer, see Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), p. 14.

5. Examples of Cayley's "color groups" may be found in Hilton's *Finite Groups* (1908). (*Cf.* Chapter VI, § 4, Ex. 1.)

6. For "Some Applications of Groups to Geometry" see R. M. Winger in *The American Mathematical Monthly*, vol. 37 (1930), pp. 1–16.

CHAPTER V

SOME GENERAL PROPERTIES OF GROUPS

32. Review. We have already (in § 11 *et aliis*) had some abstract theory of finite groups, such as the multiplication table, isomorphisms, and the Lagrange Theorem. It may be recalled that (*i*) a subgroup of index two is invariant in its group; (*ii*) all the elements of a group G that are individually invariant under some one element of G form a subgroup; (*iii*) all the elements of a group G that are individually invariant in G form an invariant subgroup called the central of G; (*iv*) if two elements each of period two have a product of period two, the two elements are commutative.

In this chapter we propose to study more properties which are independent of the mode of representing the group. We shall use G to represent a given group, H for a subgroup, p for a prime integer, and represent elements by small letters, as s and t.

33. Transforms and an Application. We may prove here abstractly what was shown by permutations in § 10; *viz.*, *An element and its transform are of the same period.* Let s of period n be transformed by t, thus giving $t^{-1}st$. Now $(t^{-1}st)^m$ equals $(t^{-1}st)(t^{-1}st)\cdots$ m times, which gives $t^{-1}s^mt$, and this $= I$ when $m = n$. Moreover, if $t^{-1}s^mt = I$ for $m < n$, we should have the impossibility $s^m = tIt^{-1}$.

Notice from $(t^{-1}st)^m = t^{-1}s^mt$ that *the mth power of a transform of s equals the transform of the mth power of s.*

Again, if $t^{-1}st = s^m$, m must be prime to the period of s.

Also if $t^{-1}st = s^m$, then $t^{-2}st^2$, which equals $t^{-1}(t^{-1}st)t$, $= t^{-1}(s^m)t$, $= s^{m^2}$; or $t^{-\alpha}\, st^{\alpha} = s^{m^{\alpha}}$. Finally, if $t^{-1}st = s^m$, then $t^{-1}s^{\beta}t$, which equals $(t^{-1}st)^{\beta}$, gives $(s^m)^{\beta}$, so that *an element that transforms s into* s^m, *transforms* s^{β} *into* $(s^{\beta})^m$.

We shall next prove the following

THEOREM. *If a group H of order h is invariant under an outside element t and the lowest power of t found in H is the mth, then H and t generate a group G,* $\equiv \{H, t\}$,* *whose order is hm.*

If $H \equiv [I, s_2, s_3, \cdots, s_h]$; then, just as in § 11, we can show that in the array

$$\begin{array}{lllll} I & s_2 & s_3 & \cdots & s_h \\ t & s_2t & s_3t & \cdots & s_ht \\ t^2 & s_2t^2 & s_3t^2 & \cdots & s_ht^2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ t^{m-1} & s_2t^{m-1} & s_3t^{m-1} & \cdots & s_ht^{m-1} \end{array}$$

there are *hm* distinct elements; also, that any *s* times a power of *t* greater than the $(m-1)$th, would be one of these *hm* elements. Finally, the group requirements are easily shown to hold.

This theorem is very useful in forming groups (*cf.* §§ 45, 46, 52); it may be stated as follows:

COROLLARY. *If a group H is invariant under the elements of a cyclic group L, then H and L generate a group* $G \equiv \{H, L\}$, *whose order is hl/c, where h, l, and c are the orders of H, L, and their cross-cut C, respectively.*

34. More About Conjugates. Bound up with the properties of transforms is the theory of conjugates, for a set of conjugates is really only a set of transforms. From the theory developed in §§ 15–17 the following theorem is obvious:

* Brackets have been used to inclose the elements of a group; we employ braces to inclose the generators of a group.

THEOREM 1. *If $s_1, s_2, \cdots, s_m$ form a complete set of conjugate elements in a group G, then the group they generate, $\{s_1, s_2, \cdots, s_m\}$, either is G itself or is the smallest invariant subgroup containing an s_i.*

DEFINITIONS. A **maximum subgroup** of a group G is one contained in no larger subgroup (other than G).

A **maximum invariant subgroup** of a group G is an invariant subgroup contained in no larger invariant subgroup (other than G).

From the preceding theorem in connection with the fact that *two invariant subgroups of a group G generate either G itself or else an invariant subgroup of G*, we have the following

THEOREM 2. *A necessary condition that an invariant subgroup H be maximum in a group G is that $\{H, s_1, \cdots, s_m\}$ equal G, where $s_1, \cdots, s_m$ is any complete conjugate set of elements in G outside H.*

Is this condition sufficient that H be a maximum invariant subgroup of G?

We conclude this section with a theorem due to Dyck.*

THEOREM 3. *If H_1 and H_2, two groups whose cross-cut is the identity, are such that each is invariant under every element of the other, then no element of either group has any conjugate except itself under the other group; in other words, each element of either group is commutative with each element of the other.*

Suppose s is any element of H_1 and that t is any element of H_2. Then $s^{-1}t^{-1}st$ when written $s^{-1} \cdot t^{-1}st$ is seen to be in H_1; when written as $s^{-1}t^{-1}s \cdot t$ it is seen to be in H_2. Since $s^{-1}t^{-1}st$ is in both groups and since their cross-cut is the identity, $s^{-1}t^{-1}st = I$. Hence, $t^{-1}st = s$, or any element of one group is seen to be commutative with every element of the other.

* *Mathematische Annalen*, vol. XXII (1883), p. 97.

COROLLARY. *In a group G if H_1 and H_2 are invariant subgroups whose cross-cut is the identity, each element of H_1 is commutative with each element of H_2.*

EXERCISES

1. Prove: The product of two transforms equals the transform of the product, all by the same element.

2. Show that the elements in the array in § 33 form a closed set, starting with the product of elements from two different rows and two different columns.

3. In the Corollary of § 33 are H and L invariant in G? Is C invariant in L and in H?

4. Prove the following generalization of the Corollary in § 33: *If H_1 and H_2 are groups of orders h_1 and h_2 respectively, and their cross-cut C is of order c, then if H_2 is invariant under each of the elements of H_1, they generate a group $G \equiv \{H_1, H_2\}$, whose order is h_1h_2/c.* For hint see Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), p. 60.

5. Change $s_1, \cdots, s_m$ in Theorem 1 of § 34 to a complete set of conjugate subgroups and prove the resulting theorem.

6. Prove: Two invariant subgroups of a group G generate G or else generate an invariant subgroup of G.

7. Prove: A necessary and sufficient condition that H be a maximum subgroup of G is that $\{H, s\}$ always equals G where s is in turn every element of G not in H.

8. Prove: The cross-cut of two invariant subgroups H_1 and H_2 of a given group G is an invariant subgroup of G.

9. What is the period of st if s and t are elements of (finite) periods m and n, respectively? (*Cf.* p. 98, Ex. 4.)

10. How many conjugates has $ab + cd$ under the symmetric group on a, b, c, d? (*Cf.* p. 15, Ex. 3.)

35. Commutators. We have already noted (§ 10) that $s^{-1}t^{-1}st$ is the commutator of the two elements s and t, and that if the commutator of every pair of elements of a group is the identity, the group is abelian, and conversely. The commutators of a group G generate or constitute a subgroup called

the **commutator subgroup.** If G and its commutator subgroup are identical, G is called a **perfect group.***

THEOREM 1. *In a group G the commutator subgroup is invariant.*

For if s is a commutator and t any element of G, we can show that t transforms s into some element of the commutator subgroup. Thus, $t^{-1}st = s(s^{-1}t^{-1}st)$, which is seen to be the product of two commutators.

COROLLARY. *A simple group of composite order is perfect.*

THEOREM 2. *The commutator subgroup of the symmetric group of degree m, $m > 1$, is the alternating group of degree m.*

The elements of the commutator subgroup are positive permutations (p. 21, Ex. 3), hence the commutator subgroup is an invariant subgroup of the alternating group. If $m > 2$ and $\neq 4$, there is no invariant subgroup whose order is > 1 and $< m!/2$, (§ 22, Th. 1). The commutator subgroup cannot be I, for then its group is abelian (this is the case if $m = 2$); hence the commutator subgroup is the alternating group of order $m!/2$. By inspection the theorem is seen to be true for $m = 2$ and $m = 4$.

COROLLARY. *The alternating group of degree m, $m > 4$, is perfect.*

We next proceed to a theorem whose proof involves some interesting work with commutators.

THEOREM 3. *In a finite group G if all those elements whose periods divide a given odd integer n are such that the commutator of every pair is commutative with its two elements, then those elements constitute an invariant subgroup.*

* From these observations evidently (i) the commutator subgroup of the direct product of two groups is the product of their commutator subgroups; (ii) the direct product of two perfect groups is itself perfect.

LEMMA 1. *If* $c = s^{-1}t^{-1}st$ *is commutative with* s, c^v *is the commutator of* s^v *and* t.

From $s^{-1}t^{-1}st = c$, we have $t^{-1}st = sc$ and $t^{-1}s^vt = (sc)^v$, which $= s^vc^v$. Whence $s^{-v}t^{-1}s^vt = c^v$.

Similarly, if c is commutative with t, c^u is the commutator of s and t^u.

More generally, if c is commutative with both s and t, c^{uv} is the commutator of s^u and t^v.

LEMMA 2. *If* $c = s^{-1}t^{-1}st$ *is commutative with both* s *and* t, $(st)^n = s^nt^nc^{-\frac{1}{2}n(n-1)}$.

From $s^{-v}t^{-1}s^vt = c^v$, $ts^v = s^vtc^{-v}$, which we use in each of the following:

$(st)^2 = st \cdot st = s \cdot ts \cdot t = s \cdot stc^{-1} \cdot t = s^2t^2c^{-1}$.

$(st)^3 = st(st)^2 = st \cdot s^2t^2c^{-1} = s \cdot ts^2 \cdot t^2c^{-1} = s \cdot s^2tc^{-2} \cdot t^2c^{-1} = s^3t^3c^{-3}$.

$(st)^4 = st(st)^3 = st \cdot s^3t^3c^{-3} = s \cdot ts^3 \cdot t^3c^{-3} = s \cdot s^3tc^{-3} \cdot t^3c^{-3} = s^4t^4c^{-6}$.

By mathematical induction we have finally

$$(st)^n = s^nt^nc^{-\frac{1}{2}n(n-1)}.$$

Similarly,

$$(ts)^n = t^ns^nc^{\frac{1}{2}n(n-1)}.$$

The proof of the theorem is now easy. For, from the preceding Lemmas, if the periods of both s and t divide an odd integer n so that $s^n = t^n = I$, then the periods of both st and ts are seen to divide n. Because from Lemma 2 we should then have $(st)^n = c^{-\frac{1}{2}n(n-1)}$ and $(ts)^n = c^{\frac{1}{2}n(n-1)}$, and from Lemma 1, $c^{\pm\frac{1}{2}n(n-1)}$ would $= I$. (How?) The set is thus closed, finite, and unique in G, hence constitutes an invariant subgroup.

From these two Lemmas we may deduce the following:

THEOREM 4. *If two elements are commutative with their commutator and have periods which divide a given odd integer* n, *they generate a group the periods of whose elements divide* n.

36. On the Quotient Group. If a group G is separated into co-sets (§ 11) as regards an invariant subgroup H, it has been pointed out that these co-sets as elements satisfy the requirements of a group (§§ 20, 21). This group Q, known as the quotient group of G as regards H, is denoted by G/H. The invariant subgroup H is sometimes called the *head*. The quotient group is illustrated at the left where G is the alternating group of degree four, and H is the four-group. Q is seen to be the cyclic group of order three. This leads us to observe in connection with general isomorphisms that *if H is any invariant subgroup of order h in G, an h:1-isomorphism can be set up between G and some other group.* This other group would be the quotient group G/H. Also, since in the separation of G into co-sets as regards H, the co-sets have the same number of elements each, the order of G equals the product of the orders of H and G/H.

I $(ab)(cd)$ $(ac)(bd)$ $(ad)(bc)$	I
(abc) (bdc) (adb) (acd)	(xyz)
(acb) (adc) (bcd) (abd)	(xzy)

The following are interesting theorems obvious from the h:1-isomorphism between G and G/H.

THEOREM 1. *If the quotient group of a group G as regards an invariant subgroup H is abelian, H contains the commutator subgroup of G.*

THEOREM 2. *The period of an element of G is divisible by the period of the corresponding element of G/H.*

THEOREM 3. *The quotient group of an abelian group G with respect to any of its subgroups is abelian.*

If the quotient group of a non-abelian group G as regards its central is abelian, G is called **metabelian.**

THEOREM 4. *In any non-abelian group the quotient group as regards the central is never cyclic.*

For if the central of G is C and G/C is a cyclic group of order m, then there must be an element s outside of C such that $G = C + Cs + Cs^2 + \cdots + Cs^{m-1}$. Whence s is commutative with every element of G, and, accordingly, is in C. But this is contrary to its choice. Hence, G/C cannot be cyclic.

In a metabelian group the central is at least of order two (why?) and the quotient group with respect to the central at least of order four (why?); and if of order four, it is the four-group.

THEOREM 5. *If H_1 and H_2, two invariant subgroups of G, have only the identity in common, and if $G/H_1 = H_2$ abstractly, then G is the direct product of H_1 and H_2.*

From § 34, Theorem 3, the elements of H_1 are individually commutative with the elements of H_2. H_1 and H_2 generate by direct product a group whose order equals the product of their two orders. (*Cf.* p. 77, Ex. 4.) But this is the order of G. Hence G is the direct product of H_1 and H_2.*

EXERCISES

1. Prove: The direct product of two (or more) simple groups of composite orders is perfect.

2. Find the commutator subgroup of the symmetric group of degree 4.

3. Prove: In a group G if each of two elements is commutative with all of its conjugates, then the commutator of these two elements is commutative with each of the two elements.

4. Prove: If s_1 and s_2 transform t into powers of itself, the commutator of s_1 and s_2 is commutative with t.

5. If $G = H + g_1H + \cdots + g_mH$ where H is a subgroup of G,

* *Cf. American Journal of Mathematics*, vol. 42 (1920), p. 125.

prove that if a co-set $g_iH(i = 1, \cdots, m)$ contains any elements of another subgroup H', it contains exactly as many of them as does H.

6. If K is a subgroup of G having only the identity in common with H which is an invariant subgroup of G, then the quotient group G/H contains a subgroup (or else itself is) simply isomorphic with K.

7. (*a*) What is the quotient group of largest order < 24 and what the one of smallest order > 1 that the symmetric group on four letters has?

(*b*) What is the quotient group of the group in Ex. 3, p. 55 as regards its subgroup of order three?

8. State and prove a converse of Theorem 1 in this Section.

9. Prove: A subgroup of index two in G contains every element of G whose period is odd. *Cf.* § 11, Th. 2; § 12, Th. 1.

10. Prove: If the quotient group of G as regards an invariant subgroup H of order h contains a subgroup K of order k, then G contains a corresponding subgroup of order kh. If K is invariant in the quotient group, the corresponding subgroup (or order kh) is invariant in G.

37. On Prime-power Subgroups. Since the alternating group of degree four contains no subgroup of order six, we see that the converse of the Lagrange Theorem in § 11 is not true in general. In the present section we propose to prove a modified converse; *viz.*,

THEOREM. *If p^m is less than and divides the order n of a group G, then G contains at least one subgroup of order $< n$ whose order is divisible by p^m (p is a prime integer).*

We shall assume the theorem true for orders $< n$, and by induction prove that it holds for n.

Let c be the order of the central C of G, and let the other elements of G be separated into complete sets of conjugates of $m_1, m_2, \cdots, m_v$ elements each. Then from § 15, Theorem 4, we have $$n = c + m_1 + m_2 + \cdots + m_v.$$

Now c is not divisible by p or else it is divisible by p.

(*i*) If c is not divisible by p, some m, say m_i, is not divisible

by p. Then G contains a subgroup (p. 42, Ex. 1) whose order n/m_1 is $< n$ and is divisible by p^m. Hence, by our assumption the theorem is proved in this case.

(*ii*) If c is divisible by p, C contains an invariant subgroup L of order p which is invariant in G,* so that G/L is of order n/p and therefore by our assumption contains a subgroup whose order is divisible by p^{m-1}. Corresponding to this subgroup, G contains a subgroup whose order is divisible by p^m (p. 82, Ex. 10).

COROLLARY 1. *If p^m divides the order n of a group G, then G contains at least one subgroup of order p^m.*

If $m = 1$, we have a minor theorem of Cauchy's, *viz.*, †

COROLLARY. 2. *If p divides the order n of a group G, G contains elements of period p.*

38. Sylow's Theorem. Of the theorems on finite groups probably the most important are Lagrange's (§ 11), Sylow's, and Cayley's (§ 12). The one yet to be considered is an extension of Cauchy's mentioned in the preceding Section, and was first proved by L. Sylow.‡ If the order n of a group G is divisible by p^m but not by p^{m+1} (p is a prime integer), then a subgroup of order p^m in G is called a **Sylow subgroup.**

SYLOW'S THEOREM. *If the order n of a group G is divisible by p^m but not by p^{m+1}, G contains at least one Sylow subgroup of order p^m, and if more than one, the total number is $\equiv 1 \pmod{p}$, and they form a single set of conjugates.*

* For by extension of the Corollary in § 33, all the elements of C whose periods are not divisible by p would not generate a group with order divisible by p. Then C must contain elements of period hp; and the hth power of such an element generates a cyclic subgroup of order p, invariant in C.

† Cauchy, *Exercises d'Analyse* (1844), III, p. 250.

‡ *Mathematische Annalen*, vol. V (1872), p. 584 *et seq.*

There are three parts to the conclusion here. The first part that G contains at least one subgroup H of order p^m follows from the Theorem of the preceding Section. We proceed to show that the total number is of the form $kp + 1$, where k is some integer. If there is only one such Sylow subgroup, $k = 0$ and H is its own conjugate, or is invariant.

LEMMA. *In G no element whose period is a power of p and which is outside the Sylow subgroup H can transform that Sylow subgroup into itself.*

For if such an element existed, it would by the Theorem of § 33 extend H to a group whose order would be a higher power of p than the mth. But this is impossible (§ 11, Lagrange's Theorem).

We shall now show that if H has any conjugates, the total number is of the form $kp + 1$. Suppose that H has at least one conjugate H_1 in G and that the cross-cut of H and H_1 is R_1 of order p^{r_1}. If we transform H_1 by the elements of H, we see by the Lemma that only the p^{r_1} elements of R_1 transform H_1 into itself. From p. 43, Ex. 6, we see, furthermore, that the elements of H transform H_1 in a set of p^{m-r_1} conjugates, all distinct and different from H. If H has any other conjugates in G, as H_2, not already found, and the cross-cut of H and H_2 is R_2 of order p^{r_2}, we obtain as before p^{m-r_2} more distinct conjugates, different from H. No one in this set could be the same as one in the preceding set; for then would $t_1^{-1}H_1t_1 = t_2^{-1}H_2t_2$ where t_1 and t_2 are elements of H. From this it would follow that $(t_1t_2^{-1})^{-1}H_1(t_1t_2^{-1}) = H_2$, which is contrary to the hypothesis that H_2 was not in the first set. On continuing we must finally have all the conjugates of H, and the number must be $1 + p^{m-r_1} + p^{m-r_2} +$ etc., in which every r is $< m$. Thus, H is in a set of $kp + 1$ conjugates.

We must yet show that G contains no Sylow subgroup of order p^m other than those conjugate to H. Suppose there were such a subgroup K. Reasoning as before we should have $lp + 1$ for the number in this set of conjugates. However, suppose instead of transforming K_1 by the elements of K, we transform K by the elements of H. If the cross-cut S of H and K is of order p^{s_1}, the number of conjugates in the set would be $p^{m-s_1} + p^{m-s_2} +$ etc. This is because H is not in the set with K. Since K cannot be in a set whose number is $\equiv 1$, (mod p), and at the same time $\equiv 0$, (mod p), K does not exist.

COROLLARY 1. *If the largest subgroup of G containing a Sylow subgroup of order p^m invariantly is of order dp^m, then G is of order $dp^m(1 + kp)$.*

Because by § 17, Th. 2, this subgroup of order dp^m is of index $1 + kp$ in G.

COROLLARY 2. *Every subgroup L of order p^l, $l < m$, is contained in at least one Sylow subgroup H of order p^m in G.*

For if L is not in some H, we could by the method used in the proof of the Theorem separate H and its conjugates into sets, using the elements of L as transforming operators. This would give $p^{m-v_1} + p^{m-v_2} +$ etc. But the number of conjugates in the set is $kp + 1$. Hence some v_i must equal m, which would mean that L is the cross-cut between itself and some Sylow subgroup of order p^m.

EXERCISES

1. Show that a subgroup of order 7 in a group G of order 35 is invariant. What can you say about the subgroups of order 5? What then about G?

2. Prove: If the order of a group is pm, where p is a prime greater

than m and m is an integer > 1, there cannot be more than one subgroup of order p.

Corollary. If the order of a group G is $2p$ where p is a prime, G contains an invariant subgroup of order p.

3. If a group G of order n contains exactly $kp + 1$ Sylow subgroups of order p^m, then $kp + 1 \leqslant n/p^m$.

4. If a subgroup of order p^ω is invariant in G, it is an invariant subgroup of every Sylow subgroup of order p^m in G.

5. By referring to p. 22, Ex. 6, show that $(p-2)! \equiv 1, \pmod{p}$, where p is a prime.

6. Prove: If in a group G every Sylow subgroup is invariant, G is the direct product of its Sylow subgroups. Hint. Use Dyck's Theorem (§ 34); start with two of the Sylow subgroups, then bring in a third, etc.

ADDITIONAL EXERCISES

1. *A major theorem of Frobenius.** Given any integer k which is a factor of the order n of a group G. The number of elements (including the identity) of G whose periods divide k is a multiple of k. See Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), § 32.

2. *A minor theorem of Frobenius.*† If p is a prime and p^α divides the order of a group G, the number of subgroups of order p^α in G is $kp + 1$. See Burnside, *Theory of Groups* (1897), § 86, or (1911), § 121.

3. If a group is perfect, has it any elements which are not commutators? Hilton, *Finite Groups* (1908), p. 233.

4. If each element (excepting the identity) of a group is of period three, show that each element is commutative with its conjugates. From Hilton, *Finite Groups* (1908), p. 62, Ex. 14.

5. For a theorem by Weisner concerning direct products see the *Bulletin of the American Mathematical Society*, vol. XXXIII (1927), p. 44.

* *Berliner Sitzungsberichte* (1895), p. 984.

† *L. c.*, p. 998.

CHAPTER VI

ON ABELIAN GROUPS

39. On the Cyclic Group. The abelian group has been defined and mentioned previously (p. 26). The importance of groups of this kind as well as the interest attached to their study justifies our devoting two or three lectures to them.

From its definition (§ 4), a cyclic group is abelian; hence, we make here some observations on cyclic groups. A cyclic group G of order n always contains at least one element of period n, which of course will generate G, and more than one such element if $n > 2$. This is because if s is of period n, then s^m $(0 < m < n)$ is always of period n if m is prime to n (which may be seen by writing s as a permutation on n letters and raising to powers according to the method of § 7), and if $n > 2$ there is always at least one such integer > 0 and $< n$. If n is a prime p, the number of such elements is $p - 1$; if $n = p^r$, the number is, from number theory, $p^r\left(1 - \frac{1}{p}\right)$; etc.*

Again, by writing s of period $k \cdot l$ as a permutation of one cycle on kl letters, we see that s^k is of period l, as also is s^{uk} if and only if u is prime to l. Notice that $s^{uk} = (s^k)^u$.

Hence, *if the integer l divides the order of a cyclic group G, (i) G has a single invariant subgroup of index l and this subgroup is cyclic; (ii) the number of elements in G of period l equals exactly the number of integers > 0 and $< l$ that are prime to l.*

If the order n of the cyclic group G equals $n_1 n_2$ where n_1 and n_2 are relatively prime, G is the direct product of two cyclic

* This number is the number of integers in a reduced residue system, (mod p^r). *Cf.* § 30.

groups of orders n_1 and n_2, respectively. (*Cf.* § 33, Corollary.)

If the order of a cyclic group G is a prime integer p, G consists of the identity and $p-1$ elements of period p.

If the order of a cyclic group G is $n = p_1^{m_1} p_2^{m_2} \cdot \cdots \cdot p_r^{m_r}$, where the p's are distinct primes and the m's positive integers, G contains an element of period $p_1 p_2 \cdot \cdots \cdot p_r$, and G is the direct product of cyclic groups of orders $p_1^{m_1}, p_2^{m_2}, \cdots, p_r^{m_r}$. (*Cf.* § 33, Corollary.)

Notes from Number Theory *

1. Reduced Residue System. If the integer m factors giving $m = p_1^{m_1} p_2^{m_2} \cdots p_r^{m_r}$ where the p's are distinct primes, then the number of integers in the reduced residue system (mod m); that is, the number of integers (including 1) > 0 and $< m$ which are prime to m, is represented by $\phi(m)$, and

$$\phi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdot \cdots \cdot\left(1-\frac{1}{p_r}\right).$$

2. Also if $m = m_1 \cdot m_2$, where m_1 is relatively prime to m_2,

$$\phi(m) = \phi(m_1) \cdot \phi(m_2).$$

3. Fermat's Minor Theorem as extended by Euler. If x is any integer prime to m,

$$x^{\phi(m)} \equiv 1, \text{ (mod } m).$$

4. Wilson's Theorem. If and only if x is a prime integer is

$$(x-1)! + 1 \equiv 0, \text{ (mod } x).$$

5. Primitive Root. Definition. If the $\phi(m)$th power of r is the smallest positive power of r congruent to 1, (mod m), r is a primitive root of m.

* *Cf.* Mathews, G. B., *Theory of Numbers*, Part I (1892), Chapter 1; Dickson, L. E., *Introduction to the Theory of Numbers* (1929), Chapters 1, 2; or any other text giving classical number theory.

6. The positive integer m has primitive roots if and only if it is 2 or 4 or p^n or $2p^n$ where p is an odd prime.

40. Subgroups of an Abelian Group. Since an abelian group is a commutative group, every one of its subgroups is not only invariant but abelian, and any of its quotient groups is abelian. In a footnote of § 37 (p. 83) we have already shown that if the order of an abelian group G is divisible by a prime p, G contains a subgroup of order p; that is, an element of period p. This may be generalized as follows:

THEOREM 1. *If the order n of an abelian group G is divisible by an integer m, G contains a subgroup of order m.*

We know that the theorem is true for small values of n. We proceed by induction to prove it true in general. Assume it true for orders $< n$. Let p be a prime factor of m, then by the observation just made, G contains an invariant subgroup H of order p. Consider now the abelian quotient group G/H. Since its order is n/p, and this is $< n$, by our assumption it contains a subgroup of order m/p, and to this subgroup of G/H corresponds a subgroup of order m in G (p. 82, Ex. 10).

From p. 86, Exercise 6, we see that

THEOREM 2. *An abelian group is the direct product of its Sylow subgroups.*

This means that if the order of an abelian group is $n = p_1^{m_1}p_2^{m_2} \cdot \cdots \cdot p_r^{m_r}$ (where the p's are distinct primes and the m's positive integers), it is the direct product of abelian groups of orders $p_1^{m_1}, \cdots, p_r^{m_r}$, respectively. Hence we study abelian groups whose orders are powers of a single prime.

THEOREM 3. *Every group of order p^2, where p is a prime, is abelian. Abstractly there are two such groups; one is cyclic,*

the other is non-cyclic and is the direct product of two groups of order p.

Evidently the group G is cyclic if it contains at least one element of period p^2. If there is no element of period p^2, there must be the identity and $p^2 - 1$ elements of period p; that is, $p + 1$ subgroups of order p. On considering the separation of these $p^2 - 1$ elements of period p into conjugate sets, we see that at least some of these elements are invariant in the group. This is because the number of elements in a conjugate set is a factor of the order of the group (§ 17, Th. 1, Cor.). If s is such an element and t is another element of G but not in $\{s\}$, then t and s generate p^2 elements, that is, G. (§ 33, Theorem.) These p^2 elements are commutative among themselves, so that all of the elements of G are invariant. Hence, no non-abelian group of order p^2 exists. The abelian groups are two in number; one cyclic, the other non-cyclic, the direct product of two groups of order p.

EXERCISES

1. If $k = 3$ and $l = 10$, use $s = (a_1 \cdots a_{10})$ to illustrate what is said in § 39 about s^k and its powers.

2. If the order of a cyclic group G is $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \cdots \cdot p_r^{m_r}$ where the p's are distinct primes and the m's positive integers, how many subgroups (including I and G) are there in G?

3. Prove: If the order of a given abelian group is not divisible by the square of any prime, the group is cyclic.

4. If G is an abelian group of order p^m (p a prime, m a positive integer) containing no element of period $> p$, how many subgroups of order p does it contain?

5. What are the Sylow subgroups in Exercise 2? What can you say about the quotient of G with respect to any one of these Sylow subgroups as head?

6. Given a non-abelian group G containing a subgroup H. If no two or more elements of H are conjugates in G, prove that H is abelian.

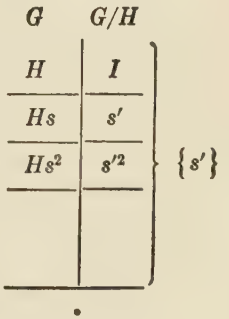
7. Discuss the possible abelian groups of order 180. Use Theorems 2 and 3 of this Section.

41. Prime-power Abelian Groups. We shall first prove

THEOREM 1. *If G is an abelian group of order p^m and s is an element of highest period in G, then G is the direct product of $\{s\}$ and a largest subgroup in G having only the identity in common with $\{s\}$. (p is a prime).**

If s is of period p^m, the theorem needs no discussion, for G is then cyclic.

Suppose s is of period p^{m_1} where $m_1 < m$. Let H be a largest subgroup of G having only the identity in common with $\{s\}$, the cyclic group generated by s. We shall employ induction in the proof. The theorem is known true for p^2 (§ 40), and we assume it true for powers of less than the mth.



Since the cross-cut of $\{s\}$ and H is I, we see from the accompanying figure that G/H contains a subgroup, $\{s'\}$, simply isomorphic with $\{s\}$. (*Cf.* p. 82, Exercise 6.) Now G/H cannot contain any element outside $\{s'\}$; for if it did, G/H would by the assumption equal the product of $\{s'\}$ and another subgroup (call it T) not I, having only I in common with $\{s'\}$. And corresponding to T there would be in G a subgroup con-

* Crelle's *Journal für die reine und angewandte Mathematik*, vol. 161 (1929), p. 255.

taining H and other elements and having only the identity in common with $\{s\}$. (P. 82, Exercise 10). But from the original hypothesis this is impossible. Hence $G/H = \{s'\}$, and by § 36, Theorem 5, G is the direct product of $\{s\}$ and H.

COROLLARY. *If G is an abelian group of order p^m and s is an element of highest period in G, then abstractly G is the direct product of $\{s\}$ and $G/\{s\}$. (p is a prime.)*

The quotient group in this Corollary is abelian and its order is a power of p. Applying the theorem to this quotient group, then to the resulting one, until the final quotient group is cyclic, we have

THEOREM 2. *An abelian group of order p^m, p a prime, is the direct product of cyclic groups.*

In this we imply not only that the elements of one cyclic group are commutative with each element of each other cyclic group, but also that any two of the cyclic groups have only the identity in common.

Our analysis has required that no one of these cyclic groups be of order greater than that of any one preceding it. That is, if $m = m_1 + m_2 + \cdots + m_r$, then $m_1 \geqslant m_2 \geqslant \cdots \geqslant m_r$. This is evidently allowable since we are dealing with direct products in which multiplication is commutative. The abelian group is said to be of order p^m and type $(m_1, m_2, \cdots, m_r)$, where $m = m_1 + \cdots + m_r$. The elements of periods $p^{m_1}, p^{m_2}, \cdots, p^{m_r}$ respectively, constitute a set of independent generators, and the integers $m_1, \cdots, m_r$ are called **invariants.** We make the following three observations:

THEOREM 3. *If two abelian groups of order p^m are of the same type (or have the same invariants), they are simply isomorphic.*

THEOREM 4. *The number of abstract abelian groups of*

order p^m equals the number of distinct integral partitions of m, each partition giving rise to a distinct type.

THEOREM 5. KRONECKER'S THEOREM. *Any abelian group of composite order is the direct product of independent cyclic groups.*

This last Theorem is among the fundamental theorems of group theory. We have named it after Kronecker because he (in 1870) gave the first explicit proof of it.

42. On the Abelian Group of Order p^m and Type (1, 1, 1, etc.). As this group is of importance in some branches of mathematics, we make two or three notes about it. There are $p^m - 1$ elements of period p. These may be separated into sets, putting into each set the $p - 1$ which together with the identity form a subgroup of order p. There are thus exactly $(p^m - 1)/(p - 1)$ subgroups of order p.

The number of independent generators is m, and each is of period p. Let us find the number of ways in which these may be chosen. For the first, s_1, there are $p^m - 1$ choices. Outside of $\{s_1\}$, there are $p^m - p$ choices for the second, s_2. For the third, $p^m - p^2$ choices, etc. The total number of choices from the group is accordingly

$$(p^m - 1)(p^m - p) \cdot \cdots \cdot (p^m - p^{m-1}).$$

If we had all these written down, some of them would be like others with the elements arranged in different order. The number of distinct sets of choices is thus

$$(p^m - 1)(p^m - p) \cdot \cdots \cdot (p^m - p^{m-1})/m!.$$

EXERCISES

1. Discuss the possible abelian groups of order p^7, where p is a prime.

2. How many abelian groups are there of order $2^5 3^4 5^7$?

3. An abelian group G is of order p^5, type (2, 2, 1), where p is a prime. In G how many elements are of period p? Of period p^2? How many cyclic subgroups are there of order p? Of order p^2?

4. In an abelian group of order p^m, type $(m_1, m_2, \cdots, m_r)$, where p is a prime and $m = m_1 + \cdots + m_r$, prove that every element is of the form $s_1^{x_1} s_2^{x_2} \cdots s_r^{x_r}$ where the s's are commutative and the period of s_i is p^{m_i}, $i = 1, \cdots, r$.

5. How many subgroups of order p^2 are there in an abelian group of order p^m, type (1, 1, etc.) $m > 1$?

ADDITIONAL EXERCISES

1. In an abelian group of order p^6, type (2, 2, 1, 1), p a prime, how many subgroups are there of type (2, 1)? *Cf.* Hilton, *Finite Groups* (1908), p. 132.

2. In an abelian group of order p^m, type (1, 1, etc.), p a prime, show that for $n < m$ the number of subgroups of order p^n is

$$\frac{(p^m - 1)(p^{m-1} - 1) \cdot \cdots \cdot (p^{m-n+1} - 1)}{(p^n - 1)(p^{n-1} - 1) \cdot \cdots \cdot (p - 1)}.$$

Burnside, *Theory of Groups* (1911), § 84.

Corollary. In an abelian group of order p^m, type (1, 1, etc.) p a prime, if $n < m$, the number of subgroups of order p^n equals the number of subgroups of order p^{m-n}.

CHAPTER VII

ON ABSTRACT DEFINITIONS AND SOME WELL-KNOWN GROUPS

43. Introduction. In any permutation group there are evidently some elements which will together generate the entire group. Thus, (abc) and (ab) generate the symmetric group of degree three. We would expect similar possibilities with the abstract representation of a group and in fact have already used $\{s\}$ to represent the cyclic group generated by s, the order being m if s is of period m; *i.e.*, if $s^m = I$. It will be recalled that by $s^m = I$ we understand that for any positive integer $x < m$, $s^x \neq I$. If there are several generators, as s_1, s_2, $\cdots$, s_r, they are said to be **independent** if no one of them can be expressed in terms of the others; that is, if $s_i (i = 1, \cdots, r)$ is not in the group generated by the other s's.

A set of generating elements defines or gives a group abstractly if we have a sufficient number of equations giving their periods and how they combine. These equations must obviously be consistent, although not of necessity independent. We could not have for example $s^2 = I$ and $s^3 = I$, for these equations are inconsistent. On the other hand $s^5 = I$ and $s^2 = s^{-3}$ are dependent.

We thus have a new viewpoint of groups. We are given a finite number of generators with equations defining their interrelations, and we proceed to study the group. More than one set of data may define the same abstract group. For example, $s^6 = I$ defines a cyclic group of order six; and $t_1^2 = t_2^3 = I$,

$t_2t_1 = t_1t_2$ also define a cyclic group of order six. In the second definition we mean the group $\{t_1, t_2\}$ generated by the elements t_1 and t_2 which are of periods 2 and 3 respectively and which are commutative.

44. Abstract Definitions of Some Well-Known Groups.

Abelian Groups. From § 40, Theorem 2, we see that the abstract definition of any abelian group can be made to depend on prime-power abelian groups, and these we know by § 41, Theorem 2, are direct products of cyclic groups. Thus, suppose the abelian group is of order 108 and contains elements of period 54 but none of period 108. Since $108 = 3^3 \cdot 2^2$, we have a Sylow subgroup of order 27 and one of order 4. The one of order 27 must be cyclic and the one of order 4 non-cyclic. The first is defined by $s_1^{27} = I$, and the second by $s_2^2 = s_3^2 = (s_2s_3)^2 = I$. This group of order 108 is thus defined by $s_1^{27} = s_2^2 = s_3^2 = (s_2s_3)^2 = I$, $s_1s_2 = s_2s_1$, $s_1s_3 = s_3s_1$.

Or, since § 41, Theorem 5, says that *any abelian group of composite order is the direct product of cyclic groups*, another definition of this abelian group of order 108 evidently is $t_1^{54} = t_2^2 = I$, $t_1t_2 = t_2t_1$.

Dihedral Groups. These groups were mentioned in § 25 where they were said to be geometrically represented by the movements of a regular n-sided polygon into itself. A dihedral group of order $2n$ may be formed by extending a cyclic group of order n by an element of period 2 which transforms each element of the cyclic group into its inverse. (See p. 68, Ex. 4). For equations we may write $s_1^n = s_2^2 = I$, $s_2^{-1}s_1s_2 = s_1^{-1}$. The last equation is equivalent to $s_1s_2s_1s_2 = I$, or $(s_1s_2)^2 = I$, so that the abstract definition is frequently written $s_1^n = s_2^2 = (s_1s_2)^2 = I$.

Dicyclic Groups. A *dicyclic group* is of order $4n$ and may

be said to be formed by extending a cyclic group of order $2n$, $n > 1$, by an element of period 4 which transforms each element of the cyclic group into its inverse and whose square is in the cyclic group. The smallest dicyclic group is seen to be of order 8; it is in fact the quaternion group (§ 31) studied by Hamilton. For equations defining the dicyclic group of order $4n$ we may write $s_1^{2n} = I$, $s_1^n = s_2^2$, $s_2^{-1}s_1s_2 = s_1^{-1}$. The last equation gives $s_1s_2s_1s_2 = s_1s_2^2s_1^{-1}$, which gives $(s_1s_2)^2 = s_1^n$ (since $s_1^n = s_2^2$). Hence the abstract definition may be written

$$s_1^{2n} = I,\ s_1^n = s_2^2 = (s_1s_2)^2.$$

A Permutation Group. If it is required to obtain abstract defining equations for a given permutation group, one way to proceed is as follows. Find certain permutations (elements) which will generate the group, then besides their periods find other relations sufficient to restrict the group they generate to the given one. If these relations are satisfied by the generating permutations, we are certain that the abstract generators give the required group. Consider, for example, the alternating group on four letters a, b, c, d. The permutations $(ac)(bd)$ and (abc) generate this group of order 12. Taking $s_1^2 = s_2^3 = I$ is not sufficient, because $\{s_1, s_2\}$ is then an infinite group containing the given group as a subgroup. (*Cf.* p. 77, Ex. 9.) Now $(ac)(bd) \cdot (abc) = (bdc)$; hence, we add $(s_1s_2)^3 = I$. The group defined by $s_1^2 = s_2^3 = (s_1s_2)^3 = I$ cannot be of order less than 12. We can readily prove that the given group is defined by these equations. For $\{s_2\}$ transforms s_1 into a conjugate set of three elements each of period 2. They are s_1, $s_2^2s_1s_2$, $s_2s_1s_2^2$. The product of the first and last is $s_1s_2s_1s_2 \cdot s_2$, which from the fact that $(s_1s_2)^3 = I$ or $s_1s_2s_1s_2 = s_2^{-1}s_1^{-1}$, equals $s_2^2s_1s_2$, the second one of the conjugates.

Hence these three elements with the identity form the four-group. From the formation of the conjugates we see that this four-group is invariant under s_2; hence this four-group and s_2 generate a group whose order is exactly 12 (§ 33, Theorem).

EXERCISES

1. Find an abstract definition for the abelian group of order p^m, type (1, 1, etc.), where p is a prime.

2. Find an abstract definition for each of the abelian groups of order 36.

3. Find an abstract definition for the abelian group of order p^6 type (3, 2, 1), where p is a prime.

4. Given $m > 1$, $n > 1$ and $s^m = t^n = I$. Show that the group generated by s and t is infinite if no other relations are imposed.

5. Show that $s_1{}^p = s_2{}^p = t^2 = I$, $s_1 s_2 = s_2 s_1$, $t^{-1} s_1 t = s_2$ define a group of order $2p^2$ (p is a prime).

6. A group of order $2n$ is defined as generated by two elements each of period two and such that their product is of period $n > 1$. Write defining equations and compare with the dihedral group of order $2n$.

7. Show that $s_1{}^2 = s_2{}^3 = (s_1 s_2)^4 = I$ defines the group of the cube (p. 68, Ex. 5), which is simply isomorphic with the symmetric group of degree four.

45. On Prime-power Groups. The present section is to develop some theory which may be of use in studying groups of a given order. Using p to represent a prime, we shall first prove a minor theorem of Sylow's.*

THEOREM 1. *In any group G of order p^m, there are at least $p - 1$ invariant elements of period p (p is a prime integer).*

Since *the number of elements in a conjugate set of elements must be a divisor of the order of the group*, any non-invariant element s_1 is here in a set of $p^{n_1} (n_1 < m)$ conjugates. Any element, s_2, not in that set, is in a set of $p^{n_2} (n_2 < m)$ conjugates; etc., no

* *Mathematische Annalen*, vol. 5 (1872), p. 584.

two sets having an element in common. Hence, the total number of non-invariants is a multiple of p. But the total number of elements other than the invariant identity is $p^m - 1$. Hence there are some invariant elements of prime-power period, all of whose powers are invariant elements.

THEOREM 2. *In any group G of order p^m, there are $kp + 1$ subgroups of index p and each such subgroup is invariant (p is a prime).*

We shall prove this theorem by induction. We know it to be true for p^2, because G is then either cyclic and there is one such subgroup or G is non-cyclic and there are $p + 1$ such subgroups (§ 40, Th. 3). Suppose the theorem holds for any group of order p^{m-1}. In G of order p^m there is by the preceding Theorem an invariant subgroup H of order p. With H as head we obtain a quotient group Q of order p^{m-1}. Corresponding to each of the $k_1p + 1$ subgroups of order p^{m-2}, which are invariant in Q, there is an invariant subgroup of order p^{m-1} in G (p. 82, Ex. 10), and containing H. No other subgroup of order p^{m-1} in G could contain H, for then we would have more than $k_1p + 1$ subgroups of order p^{m-2} in Q. Since H is of order p, any subgroup of G either contains all of H or else contains only the identity in common with it. We see that we have yet to consider subgroups of order p^{m-1} in G which have only the identity in the head H. Such a subgroup will then have exactly one element in each of the following co-sets (*cf.* p. 81, Ex. 5), and hence be simply isomorphic with Q. If there is at least one such subgroup S, there are exactly p^n, where n is the number of elements in a set of independent generators of Q. Because, if s generates H and if $t_1, t_2, \cdots, t_n$ are independent generators of S, we get a group simply isomorphic with Q by

choosing as generators: one element from st_1, s^2t_1, $\cdots$, s^pt_1; one from st_2, $\cdots$, s^pt_2; $\cdots$; one from st_n, $\cdots$, s^pt_n. Since s and S are invariant in G (*cf.* § 36, Th. 5), each of the p^n subgroups is invariant. The total number is thus $p^n + k_1p + 1$, or $kp + 1$.

Using the same notation we see that since Q contains an invariant subgroup of order p, G contains an invariant subgroup of order p^2. If this is true in general, then Q contains an invariant subgroup of order p^2, and corresponding to it G contains an invariant subgroup of order p^3. (See the accompanying skeleton diagram for quotient groups when $p = 3$.) Continuing we arrive at the following

THEOREM 3. *In any group G of order p^m (p a prime) there is at least one invariant subgroup of order p^i, $i = 1, 2, \cdots, m - 1$.*

COROLLARY. *In any group G of order p^m (p a prime) there is a series of invariant subgroups starting with one of order p^{m-1} and going to the identity, each being of index p in the preceding.*

THEOREM 4. *In a group G of order p^m, where p is an odd prime, if every subgroup is invariant, G is abelian.*

From Theorem 1 all elements of period p must be invariant. We shall use induction in the proof. The theorem is known true for $m = 2$. Assume it true for $m - 1$. With a subgroup H of order p, generated by c of period p, as head we obtain a quotient group Q of order p^{m-1} every subgroup of which must be

invariant since the corresponding one in G is invariant. Then by our assumption Q is abelian, and hence the commutator subgroup of G is in H.

We shall now show that the assumption of the existence of a non-invariant element in G leads to a contradiction. Suppose s of period p^a non-invariant in G and such that there is no non-invariant element of greater period. Let t of period p^β be an element of lowest period not commutative with s. Then $a \geqslant \beta > 1$. Since Q is abelian, s is not transformed out of its coset by t; that is, $t^{-1}st = s$ times a power of c. Since $\{s\}$ is cyclic and invariant under t, $t^{-1}st =$ a power of s. Hence, the p^{a-1}th power of s generates H. Similarly a $p^{\beta-1}$th power, of t generates H. Accordingly, $t^{p^{\beta-1}} = s^{kp^{a-1}}$. We shall now show that $ts^{-kp^{a-\beta}}$, which obviously is not commutative with s, is of lower period than is t. Raising to the $p^{\beta-1}$th power, we have by Lemma 2 of § 35 $t^{p^{\beta-1}}s^{-kp^{a-1}}$ times the commutator of these factors to a power divisible by the odd prime p. This equals $t^{p^{\beta-1}} \cdot t^{-p^{\beta-1}}$, which $= I$. Hence, the assumption leads to a contradiction. Therefore G must be abelian.

46. An Application. We shall now use any theory at our disposal and in particular Sylow's Theorem to determine all the distinct abstract groups of order p^3 and all those of order 12.

Abstract Groups of Order p^3. There are easily seen to be three abelian groups of order p^3 (p a prime), their types being (3), (2, 1), and (1, 1, 1), respectively (§ 41, Th. 4). For the non-abelian groups we first discuss the case for $p = 2$, then the case for p an odd prime.

A non-abelian group of order 2^3 must have an element of period greater than 2 (p. 27, Ex. 10) and cannot have one of period 8. Hence, there is a cyclic subgroup of order 4, which is

invariant (§ 11, Th. 2). If s generates this subgroup, $s^4 = I$; and furthermore any element, as t, outside $\{s\}$ and in G must have its square in $\{s\}$ (by Th. of § 33) and its period cannot be different from 2 or 4. Nor can t be commutative with s. The only element into which s can be transformed is s^{-1}. From § 44, if $t^2 = I$ and $t^{-1}st = s^{-1}$, we know we have the dihedral group of order 8; if $t^2 = s^2$ and $t^{-1}st = s^{-1}$, we know we have the dicyclic group of order 8 (quaternion group).

A non-abelian group of order p^3, p an odd prime, may have an element of period p^2 or may have no elements of period $> p$. Consider the possibility of a group G containing an element s of period p^2. From § 45, $\{s\}$ will be invariant in G; and since G is non-abelian, an outside element, as t, cannot be commutative with s. But t must transform $\{s\}$ into itself and t^p must be in $\{s\}$ (by Th. of § 33). Hence under t the elements of $\{s\}$ must be transformed in sets of conjugates, p in a set. Accordingly, t may transform s into s^{p+1} or into s^{2p+1} or into s^{3p+1}, etc. It is sufficient to use $t^{-1}st = s^{p+1}$,* for then $t^{-2}st^2 = s^{p^2+2p+1}, = s^{2p+1}$; $t^{-3}st^3 = s^{3p+1}$; etc. Now ts^i transforms s just as t does. Furthermore, outside of $\{s\}$ G contains elements of period p and elements of period p^2. For if $t^{p^2} = I$ and $t^p = s^{ap}$, then $s^{-a}t$ is easily shown to be of period p; or if $t^p = I$, then st is easily shown to be of period p^2. Suppose t of period p, then we have for abstract definitions of this group $s^{p^2} = t^p = I$, $t^{-1}st = s^{p+1}$.

Consider, finally, the possibility of a group G which is non-abelian and has no elements of period $> p$. From the preceding section there must be a subgroup made up of the identity

* t^{-1} st could not be s^{p+n} where $n \not\equiv 1 \pmod p$, for this would give $t^{-p}\, st^p = s^{(p+n)^p}$ and we know that t^p is commutative with s. Hence, $(n+p)^p \equiv 1 \pmod{p^2}$, or $n^p \equiv 1 \pmod{p^2}$. But from Fermat's Theorem (*cf.* § 39) in number theory $n^{p-1} \equiv 1 \pmod p$, or for all values of n we have $n^p \equiv n \pmod p$. Hence n^p can be $\equiv 1 \pmod p$, only when $n \equiv 1 \pmod p$.

and $p-1$ invariant elements of period p, and this cyclic subgroup must be contained in another subgroup H of order p^2 which is abelian (§ 40, Th. 3), non-cyclic, and invariant in G (§ 45, Th. 2). Suppose s_1 is invariant in G and that $H = \{s_1, s_2\}$ where $s_1^p = s_2^p = I$, $s_1 s_2 = s_2 s_1$. An element, t, outside H must be of period p and must be commutative with s_1 but not with s_2; nor can t transform s_2 into its own powers. Why? Now H contains p subgroups of order p besides $\{s_1\}$, and s_2 generates one of these; others are generated by $s_1 s_2$, $s_1^2 s_2$, $\cdots$, $s_1^{p-1} s_2$. The only transformations t can effect are obviously among these subgroups, so that we have $t^{-1} s_2 t = s_1 s_2$. Hence G is defined by $s_1^p = s_2^p = t^p = I$, $s_1 s_2 = s_2 s_1$, $s_1 t = t s_1$, $t^{-1} s_2 t = s_1 s_2$.

Abstract Groups of Order 12. Abelian groups of order 12 are the direct products of abelian Sylow subgroups of orders 3 and 4 (§ 40, Th. 2); and since there are two abelian groups of order 4, we have two abelian groups of order 12, one cyclic and one non-cyclic.

For non-abelian groups of order 12 we note first by Sylow's theorem that there are subgroups of orders 4 and 3; one or three of order 4 and one or four of order 3. There cannot be one of order 4 and one of order 3 for then these would be invariant and the group a direct product and hence abelian; nor can there be three of order 4 and four of order 3. Why? Hence we have two cases to study: one subgroup of order 4 and four of order 3; one subgroup of order 3 and three of order 4. The group contains elements of periods 3 and 2. If there is but one subgroup H of order 4, it is invariant and an outside element, as t, must transform the elements of H among themselves and this in a set of three because the period of t is 3. Hence H must be the four-group, and G is simply isomorphic with the alternating group of degree 4.

In the second case, there must be an invariant subgroup of order 3, say S, generated by s where $s^3 = I$. Let H_1, H_2, H_3 be the three conjugate subgroups of order 4. Use the elements of H_2 to transform H_1. As many must transform it into itself as transform it into H_3 and these transforming H_1 into itself must form a subgroup. (*Cf.* p. 43, Ex. 6.) This subgroup then consists of the identity and an element of period 2. This element t of period 2 must be in H_1; otherwise $\{H_1, t\}$ would be a subgroup of order 8, which is impossible. Similarly, t is in H_3. The conjugate set H_1, H_2, H_3 generates G. Hence G contains t as an invariant element. (*Cf.* § 17, Th. 3, Cor.) Then s and t generate a cyclic subgroup of order 6, which is invariant in G (§ 11, Th. 2). This cyclic subgroup extended by an outside element whose square is in it must give the group of order 12. The outside element can be of no period excepting 2 or 4. There are just these two possibilities then and each gives a known group. One gives the dihedral group of order 12, the other the dicyclic group of order 12. We have found a total of 5 groups of this order, 2 abelian and 3 non-abelian.

47. Hamiltonian Groups. A non-abelian group in which every subgroup is invariant was called by Dedekind a **Hamiltonian group.** The smallest such group is the quaternion group, which we have already seen was also dicyclic. From this definition it follows that any subgroup of a Hamiltonian group is itself Hamiltonian or else abelian; also, a Hamiltonian group is the product of its Sylow subgroups. Another observation is that in a Hamiltonian group an element of period two is invariant. From § 45, Theorem 4, we have

THEOREM 1. *A group of order p^m, where p is an odd prime, is never a Hamiltonian group.*

We shall now proceed to prove a theorem about direct products.

THEOREM 2. *The direct product G of a quaternion group and one or both of the following abelian groups — an abelian group of order 2^m, type (1, 1, etc.) and an abelian group of odd order, is a Hamiltonian group.*

Let Q represent the quaternion group and A the abelian factor of G. As every subgroup of A and of Q is invariant in G, we have only to consider subgroups generated by elements from both Q and A. Any element of A is invariant in G and an element of Q is transformed into itself or else into its inverse by any element of G. Hence any subgroup generated by elements from Q and A is invariant in G.

EXERCISES

1. Prove: The number of elements in a conjugate set of elements is a divisor of the order of the group.

2. Study the non-abelian groups of order 30.

3. Show that every subgroup of the quaternion group $s_1^4 = I$, $s_1^2 = (s_1 s_2)^2 = s_2^2$ is invariant.

4. If p and q are primes and $p > q$, show that there is always a cyclic group of order pq; and if $p - 1$ is divisible by q, at least one non-abelian group of order pq.

5. Is the direct product of two quaternion groups having only the identity in common a Hamiltonian group?

ADDITIONAL EXERCISES

1. $(ab)(cd)$ and (ace) generate the alternating group on the five letters a, b, c, d, e. Now $(ab)(cd)\cdot(ace) = (abcde)$. Show that $s_1^2 = s_2^3 = (s_1 s_2)^5 = I$ define this group of order 60. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), § 58.

2. Make out a table showing the number of abstract groups for each possible order less than 32. *Cf.* Easton, *Constructive Development*

of Group Theory (1902), p. 77 or Burnside, *Theory of Groups* (1911), p. 161.

3. One of the fifteen abstract groups of order 24 contains no subgroup of order 12, and it is accordingly sometimes called the *non-twelve group of order* 24.* Verify that this group is defined by $s_1^3 = s_2^2$, $s_2^4 = (s_1 s_2)^3 = I$. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), p. 154.

4. Prove the converse of the Theorem of § 47, a Theorem of Miller's: Any Hamiltonian group is the direct product of a quaternion group and one or both of the following groups: an abelian group of order 2^m, type (1, 1, etc.) and an abelian group of odd order. *Cf.* Hilton, *Finite Groups* (1908), p. 178.

* Miller, G. A., *Transactions of the American Mathematical Society*, vol. 8 (1907), p. 5.

CHAPTER VIII

THE GROUP OF ISOMORPHISMS AND THE COMPOSITION-SERIES

THE GROUP OF ISOMORPHISMS

48. Examples and Definitions. The idea of isomorphism was introduced early (§ 20) and has already been much used in some Chapters. Here, we are to study the 1:1-isomorphism of a group with itself, sometimes called an **automorphism.** Evidently any group can be put into simple isomorphism with itself and usually in several different ways; and for a finite group in only a finite number of ways. For an example, automorphisms of the abelian group of order 8 and type (2, 1) are shown.

I	*I*	*I*
a (1234)	*d* (1234)(56)	*a* (1234)
(13)(24)	(13)(24)	(13)(24)
b (1432)	*f* (1432)(56)	*b* (1432)
c (56)	*e* (13)(24)(56)	*e* (13)(24)(56)
d (1234)(56)	*b* (1432)	*f* (1432)(56)
e (13)(24)(56)	*c* (56)	*c* (56)
f (1432)(56)	*a* (1234)	*d* (1234)(56)

Of course the identity always corresponds to itself. Any element or any subgroup, as the central, that corresponds to itself in every automorphism of its group is said to be **characteristic.** Besides the identity the common square of the elements of period 4 is characteristic in the example. By placing letters before the elements, permutations can be obtained which show exactly what the automorphism is, or in other words, what transformation has been made upon the original

arrangement (left hand one here) to give the new one. No letter is needed before a characteristic element. Here, $\begin{pmatrix} abcdef \\ dfebca \end{pmatrix}$, or $(adbf)(ce)$, gives the first transformation, and $\begin{pmatrix} abcdef \\ abefcd \end{pmatrix}$, or $(ce)(df)$ gives the second. By using the two-line permutations it is not difficult to see that the product $\begin{pmatrix} abcdef \\ dfebca \end{pmatrix}\begin{pmatrix} abcdef \\ abefcd \end{pmatrix} = \begin{pmatrix} abcdef \\ fdcbea \end{pmatrix}$ gives an automorphism. Thus, remembering that b stands for (1432), c for (56), etc., the product $b \cdot c$ is f. We must show that in the correspondence indicated by $\begin{pmatrix} abcdef \\ fdcbea \end{pmatrix}$ the product $d \cdot c$ is a. Since $b \cdot c$ is f, we know from $\begin{pmatrix} abcdef \\ dfebca \end{pmatrix}$ that $f \cdot e$ is a; and then from $\begin{pmatrix} abcdef \\ abefcd \end{pmatrix}$ that $d \cdot c$ is a. Accordingly, from what we know about permutations (*cf.* §§ 6, 9), the set of permutations indicating the automorphisms of a group G, themselves form a group which abstractly is known as the **group of isomorphisms of G.*** Since this group of isomorphisms can be written as a permutation group on $m - c$ letters, where m is the order of G and c the number of its characteristic elements, it is a subgroup of the symmetric group of order $(m - c)!$. We can sometimes determine the order of the group of isomorphisms of a group by studying the choices and correspondences of a set of generators. In the example, G is generated by any element of period 4 and one of the non-characteristic elements of period 2. Thus, to (1234) can correspond any one of four elements, and

* Sometimes called the *group of automorphisms of G.*

simultaneously to (56) either of two elements. Hence, the order of the group of isomorphisms is 8. Here $(adbf)(ce)$ and $(ce)(df)$ generate a dihedral group of order 8, which is therefore the group of isomorphisms of this abelian group of order 8, type (2, 1).

In a non-abelian group some of the automorphisms can be effected by transforming the group by some of its own elements. Such isomorphisms are known as **inner,** in contradistinction to all others which are known as **outer isomorphisms.*** As an example we may use the symmetric group on the three letters a, b, c. Transforming

I	I	I
(abc)	(abc)	(acb)
(acb)	(acb)	(abc)
(ab)	(bc)	(ab)
(ac)	(ab)	(bc)
(bc)	(ac)	(ac)

by (abc) gives the second writing; again, transforming (the original) by (ab) gives the third writing; etc. Here there are six inner isomorphisms (counting the identical); moreover, the group of isomorphisms of this group is only of order six (there are two choices for a generator of period 3 and three choices for the independent generators of period 2). Hence, there are no outer isomorphisms. This is what is called a **complete group,** which is one whose central is the identity and which admits of no outer isomorphism.

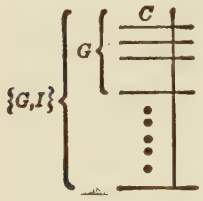
We might point out that the symmetric group on the three letters a, b, c consists of all the permutations on these letters under which the group $[I, (abc), (acb)]$ is invariant, and is therefore the holomorph of the cyclic group of order 3. In

* *Cogredient* and *contragredient* are sometimes used instead of *inner* and *outer*.

general the **holomorph** of a regular group G of degree m is the group consisting of all the permutations on those m letters under which G is invariant.

49. Inner and Outer Isomorphisms. First, *the group of inner isomorphisms of a group G is abstractly G/C, where C is the central of G.* For, if $G \equiv C + Ct_1 + Ct_2 +$ etc., all the elements in a co-set transform G into the same automorphism. To show that t_1 and t_2 from different co-sets transform G into different automorphisms, suppose the contrary. Then $t_1^{-1}xt_1 = t_2^{-1}xt_2$, as x is in turn each of the elements of G. From this we have that $t_2t_1^{-1}x = xt_2t_1^{-1}$, giving $t_2t_1^{-1}$ as an invariant element of G, and hence in C. Then Ct_1 would contain t_2, which is contrary to assumption.

Second, *the group of inner isomorphisms of a group G is an invariant subgroup of the group of isomorphisms of G.* If I represents the group of isomorphisms of G and C is the central of G, then in the group $\{G, I\}$ evidently C is invariant (since characteristic in G). Moreover I is simply isomorphic with $\{G, I\}/C$. Why? And since G is invariant in $\{G, I\}$, the corresponding subgroup of $\{G, I\}/C$ is invariant. (See accompanying diagram.) But this is seen to be G/C. Hence abstractly the group of inner isomorphisms of a group G is an invariant subgroup of the group of isomorphisms of G.



EXAMPLE. Illustrate the two propositions of this Section using for G the dihedral group of order 8.

50. On Automorphisms of Abelian Groups. Suppose s is a generator of a cyclic group G of order m. From § 39 and Notes (p. 88) we know that G has exactly $\phi(m)$ elements of

period m, each a power of s, and hence the group of isomorphisms of G is of order $\phi(m)$. This group of isomorphisms is readily shown to be abelian. Thus, if $t_1^{-1}st_1 = s^{n_1}$ and $t_2^{-1}st_2 = s^{n_2}$, then $(t_1t_2)^{-1}s(t_1t_2) = s^{n_1n_2}$, and likewise $(t_2t_1)^{-1}s(t_2t_1) = s^{n_1n_2}$; hence $t_1t_2 = t_2t_1$.

A very simple example may be of help. We see that for $m = 5$ there are $\phi(5) = 4$ elements of period 5. Moreover, since 5 is of the form p^n, some integer in the reduced residue system (mod 5), is a primitive root (p. 89). Here 2 is a primitive root. Then if $s^5 = I$ and $t^{-1}st = s^2$, the powers of t give all the isomorphisms of the group $\{s\}$. We show here the resulting automorphisms.

I	I	I	I
$(abcde)$	$(acebd)$	$(adbec)$	$(aedcb)$
$(acebd)$	$(aedcb)$	$(abcde)$	$(adbec)$
$(adbec)$	$(abcde)$	$(aedcb)$	$(acebd)$
$(aedcb)$	$(adbec)$	$(acebd)$	$(abcde)$

The group of isomorphisms is accordingly not only abelian here but cyclic, and is of order 4. It is worth while to notice that this is a regular group and that the permutations transforming the original arrangement into each of the three following are: $(bced)$, $(bdec)$, and $(be)(cd)$, respectively. If a cyclic group is written as a regular group, we see that it is always possible to write the transformation for any automorphism. It is not as easy to find such a transforming operator if the group has more than one generator.

We thus see that if the order of a cyclic group is an odd prime p, its group of isomorphisms is a cyclic group of order $p - 1$; or more generally, if the order of a cyclic group is $2p^n$ or p^n(p an odd prime), its group of isomorphisms is a cyclic group of order $p^{n-1}(p - 1)$. This is because for these powers and these

alone there is a primitive root r (mod $2p^n$ or p^n), such that for $s^{2p^n} = I$ or $s^{p^n} = I$ we have $t^{-1}st = s^r$, and the $p^{n-1}(p-1)$ powers of t give all the automorphisms of the group.

If the order of a cyclic group is 2^n, $n > 2$, it can be shown that its group of isomorphisms is an abelian group of order 2^{n-1}, type $(n-2, 1)$. See p. 123, Additional Ex. 3.

Prime-power Abelian Groups. If a non-cyclic abelian group is of order p^m, there are several subgroups of each possible order instead of just one of each order as found in the cyclic group. Except for a few very special types the study of the group of isomorphisms is involved, although formulas for the order have been developed by both Ranum * and Miller.†

Direct Products. If a group G is the direct product of characteristic subgroups which have only the identity in common, the group of isomorphisms of G is the direct product of the groups of isomorphisms of these characteristic subgroups. G may be abelian or non-abelian. Since each such subgroup is characteristic, it must correspond to itself in each automorphism of G; and because G is their direct product, their automorphisms determine the automorphisms of G, and each can have all its own possible automorphisms. Thus, suppose G is the direct product of a symmetric group of degree three, G_6, and a dihedral group G_{10} of order 10 (formed by extending a cyclic group of order 5 by the proper element of period 2). The subgroup of order 3 in G_6 is unique in G and hence characteristic, and similarly for the subgroup of order 5 of G_{10}. Again the elements of period 2 in G that are invariant individually

* Ranum, *Transactions of the American Mathematical Society*, vol. 8 (1907), p. 83.

† Miller, *Bulletin of the American Mathematical Society*, vol. 20 (1914), p. 364.

under elements of period 5, are those of G_6; hence G_6 is characteristic, and similarly G_{10} is characteristic. Moreover, each may take on all of its automorphisms independent of the other. Hence, the group of isomorphisms of G is the direct product of the groups of isomorphisms of G_6 and of G_{10}.

Abelian Groups. The direct product theory gives us here: *The group of isomorphisms of an abelian group is the direct product of the groups of isomorphisms of its Sylow subgroups.* Thus, if G is the direct product of the non-cyclic group of order 4 and the cyclic group of order 5, its group of isomorphisms is the direct product of a symmetric group of order 6 and a cyclic group of order 4. It may be unnecessary to add that this theorem does not cover the case of an abelian group of order p^2, type (1, 1) even though this group is the product of two cyclic groups of order p. Why? The order of the group of isomorphisms in this case is $(p^2 - 1)(p^2 - p)$.

EXERCISES

1. Show that the group of isomorphisms of an octic group G is simply isomorphic with G. Is this group then complete?

2. Find the group of isomorphisms of the alternating group on four letters. What is the group of inner isomorphisms of this alternating group?

3. What is the order of the group of isomorphisms of an abelian group of order p^m, type (1, 1, etc.)? (*Cf.* § 42.)

4. Show that the group of isomorphisms of an abelian group of order p^m, type (1, 1, etc.), can be written as doubly transitive if $p = 2$, but only simply transitive if p is an odd prime.

5. Find the group of isomorphisms of the direct product of a non-cyclic group of order 4 and a cyclic group of order 9.

6. Use Theorem 5 of § 17 to prove that the order of the holomorph of a cyclic group of order p, p being any prime integer, is $p(p - 1)$.*

* *Cf.* Miller, G. A., *American Journal of Mathematics*, vol. 44 (1922), p. 122.

51. Additional Theory. From what has been noted in the preceding section we see that *a necessary and sufficient condition that the group of isomorphisms of an abelian group G be cyclic is that G be cyclic and of order 4 or p^n or $2p^n$ where p is an odd prime and n a positive integer.*

We give next a theorem of Miller's: *A necessary and sufficient condition that the group of isomorphisms of an abelian group G be abelian is that G be cyclic.** The sufficiency is covered by what has already been said. We shall show that G is necessarily cyclic. For if G is non-cyclic, it must contain some non-cyclic Sylow subgroup. Let s_1 and s_2 be two independent elements of highest period in this Sylow subgroup. The automorphism indicated by

$$t_1^{-1}s_1t_1 = s_1^k (k > 1),\ t_1^{-1}s_2t_1 = s_2$$

is non-commutative with

$$t_2^{-1}s_1t_2 = s_1s_2,\ \ t_2^{-1}s_2t_2 = s_2;$$

because $$(t_1t_2)^{-1}s_1(t_1t_2) = s_1^k s_2^k$$

while $$(t_2t_1)^{-1}s_1(t_2t_1) = s_1^k s_2,$$

so that $$t_1t_2 \neq t_2t_1.$$

Again, *a sufficient condition that an element be invariant in the group of isomorphisms of an abelian group is that it transform every element of G into the same power of itself.* For if x takes on as values the different elements of G and $t_1^{-1}xt_1 = x^n$ while $t_2^{-1}xt_2 = y$, where y is an element of G not necessarily x^n, then $(t_1t_2)^{-1}x(t_1t_2) = y^n$ and $(t_2t_1)^{-1}x(t_2t_1) = y^n$. Hence, $t_1t_2 = t_2t_1$.

The order of the holomorph of a group G equals the product of the order of G and the order of the group of isomorphisms of G. If G is written as a regular permutation group of order and

* *Cf.* Miller, G. A., *Transactions of the American Mathematical Society*, vol. 1 (1900), p. 397.

degree n, every permutation of its holomorph H transforms G into identical correspondence (each element into itself) or else according to some of its other automorphisms. By Jordan's Theorem (p. 32) the permutations transforming each of the elements of G into itself constitute a subgroup of order n in H and each of these permutations is commutative with the elements of the group of isomorphisms of G, and the two have only the identity in common. Hence the theorem is proved. (*Cf.* p. 77, Ex. 4.)

EXAMPLES. Since the order of the group of isomorphisms of the non-cyclic group of order 4 is six, the holomorph of the non-cyclic group of order 4 is of order 24. Since I, $(ab)(cd)$, $(ac)(bd)$, $(ad)(bc)$ is unique in the symmetric group on a, b, c, d, the holomorph is easily seen to be this symmetric group.

Again, the holomorph of the cyclic group of order 5 is of order 20. Referring to § 50 we see that this holomorph is given by $(abcde)$ and $(bced)$.

More generally, we see that if a cyclic group C of order n is written as a regular permutation group of degree n, its holomorph can be obtained by extending C by permutations on the same letters which effect all its automorphisms.

Another theorem of Miller's is used in closing this section.*

The group of isomorphisms of a dihedral group G of order $2n$ formed from a cyclic group C of order n, $n > 2$, is the holomorph of C.

C is unique in G and hence characteristic. The elements of G outside C are of period 2. Any automorphism of G can be formed by choosing a generator of C and then independently any one of the n elements of period 2. There are no other automorphisms; hence the order of the group of isomorphisms

* *Cf.* Miller, *Philosophical Magazine*, Sixth Series, vol. 15 (1908), p. 224.

of G equals the order of the holomorph of C. Also, if n letters were used before the n elements of period 2 (outside of C), we should see that the group of isomorphisms of G could be represented transitively on n letters. If G is generated by s and t, where s of period n generates C, and $t^{-1}st = s^{-1}$; and if t_1 transforms every element of C into itself and t into ts, we have $t_1^{-1}st_1 = s$ and $t_1^{-1}tt_1 = ts$. This shows that t_1 is of period n. On the n letters placed before the n elements of period 2 in G, this cyclic subgroup would be regular and transitive; and this cyclic subgroup is unique in the group of isomorphisms on the n letters, and hence invariant.

We have shown that the group of isomorphisms of G is of the same order as is the holomorph of C, that it contains an invariant cyclic subgroup of order n, and that it can be written transitively on n letters. Accordingly, by the definition of the holomorph of a regular group, this group of isomorphisms must be simply isomorphic with the holomorph of C.

52. Two Applications. A Proof of Wilson's Theorem.* We proceed to use some group theory to prove that *if and only if x is a prime integer is* $(x-1)! \equiv -1 \pmod{x}$. (See § 39.)

If x is an odd prime integer (the case $x = 2$ is trivial), the group of isomorphisms of the cyclic group of order x is a cyclic group of order $x - 1$, an even integer. Since the product of the elements of a cyclic group of even order is its element of period 2, the product of the elements of the congruence group $1, 2, \cdots, (x-1), \pmod{x}$, is congruent to $-1 \pmod{x}$.

On the other hand if x is not prime but is > 4 (by trial the congruence is seen to fail for $x = 4$), the group of isomorphisms of the cyclic group of order x is an abelian group of order $\phi(x)$,

* *Cf.* Miller, *Annals of Mathematics*, Second Series, vol. 4 (1903,) p. 188.

representable as a congruence group by the reduced residue system (mod x). The product of the $\phi(x)$ elements of this abelian group is one of its elements of period 2 if $\phi(x)$ is even, is $+1$ if $\phi(x)$ is odd. The product of the $x - 1 - \phi(x)$ integers not relatively prime to x evidently is $\equiv 0 \pmod{x}$. Hence the product $(x-1)!$ is not $\equiv -1 \pmod{x}$.

Formation of New Groups. Not infrequently a group G is formed by extending a given group H by an element t under which H is invariant. A dihedral group is an example, for there a cyclic group is extended by an element of period 2 which transforms every element of the cyclic group into its inverse. The generalized dihedral group (any abelian group containing an element of period greater than 2 extended by an element of period 2 which transforms each element of the given abelian group into its inverse) is another example. The group of isomorphisms of the basic group H is thus of importance, since from it we would know how H could be transformed into itself.

I
$(abcdefg)$
$(acegbdf)$
$(adgcfbe)$
$(aebfcgd)$
$(afdbgec)$
$(agfedcb)$

Thus, we may take the cyclic group of order 7 (shown at the right) and instead of extending by $(bg)(cf)(de)$ which transforms each element into its inverse and would give the dihedral group of order 14, we may select $(bce)(dgf)$ which transforms each element into its square. The group which is formed is of order 21.

EXERCISES

1. Prove: The product of all the elements of an abelian group G is the identity if G is of odd order, is a characteristic element of period 2 if G is of even order.

2. Assuming that a necessary and sufficient condition that an element be invariant in the group of isomorphisms of an abelian group G is that it transform every element of G into the same power

of itself,* discuss the central of the group of isomorphisms of the direct product G of the four-group and a cyclic group of order 9. (*Cf.* p. 113, Ex. 5.)

3. Show that the group of isomorphisms of a dicyclic group G formed by extending a cyclic group C of order > 4, is the holomorph of C.†

4. By considering the group of isomorphisms of a cyclic group of order m, discuss Euler's extension of Fermat's minor theorem: $x^{\phi(m)} \equiv 1 \pmod{m}$, where x is any integer prime to m.‡ Hint. p. 70, Example Two.

5. Discuss the group formed by extending $\{s\}$ where $s^5 = I$ by an element of period 4 from its group of isomorphisms. (*Cf.* § 50.)

6. Discuss the groups of order pq where p and q are distinct primes. (*Cf.* p. 105, Exercise 4.)

THE COMPOSITION-SERIES

53. Definitions and Examples. The symmetric group of degree 4 contains the alternating group of degree 4 as a maximum invariant subgroup (§ 34); this latter contains the four-group as a maximum invariant subgroup, and this a group of order 2 as a maximum invariant subgroup, and this the identity. This illustrates the **composition-series** of a group G, which is a complete set of subgroups each a maximum invariant subgroup of the preceding one in the set. The relations of the various groups may be seen from the diagram on page 119.

If G, H_1, H_2, H_3, $\cdots$, H_n constitute the composition-series of G, the quotient groups, G/H_1, H_1/H_2, $\cdots$, H_{n-1}/H_n, H_n are a set of **composition-factor-groups** of G whose orders are

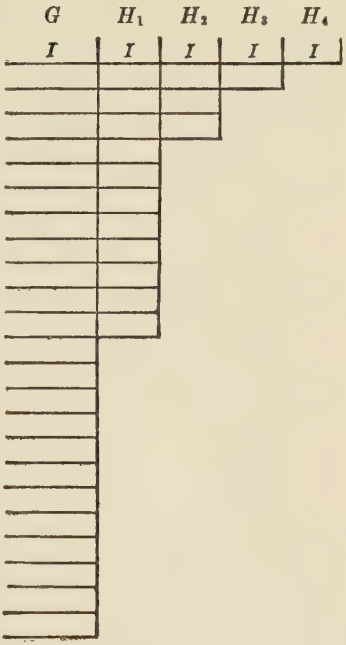
* *Cf.* Miller, *Transactions of the American Mathematical Society*, vol. 2 (1901), p. 260.

† This and the corresponding theorem on a dihedral group are included in a more general theorem by the author in the *Transactions of the American Mathematical Society*, vol. 19 (1918), pp. 331–40.

‡ *Cf.* Miller, *Annals of Mathematics*, Second Series, vol. 2 (1900–1901), p. 77.

the **composition-factors** of G. Thus, in the illustration the composition-factors are 2, 3, 2, 2, and the composition-factor-groups are the cyclic groups of these respective orders.

For another example suppose G is a cyclic group of order 30. We may have for one composition-series cyclic groups of orders 30, 15, 3, 1, or of orders 30, 10, 5, 1. For the former the composition-factors are 2, 5, 3, for the latter 3, 2, 5.



Observations. 1. When complete, a composition-series terminates with the identity.

2. A group may have more than one composition-series, but probably the composition-factors are always the same excepting as to arrangement.

3. Not every subgroup of a composition-series is necessarily invariant in the given group. Example. H_3 in the first illustration.

4. The composition-factor-groups are simple. For if H_i/H_{i+1} has an invariant subgroup, H_{i+1} is contained in an invariant subgroup (other than H_i) in H_i (p. 82, Ex. 10).

5. The product of the composition-factors equals the order of the group.

54. The Jordan-Hölder Theorems. In the preceding sec-

tion it was suggested that for a given group the composition-factors were always the same excepting possibly in arrangement. This proposition was first proved by M. Jordan,* but follows from a theorem of Hölder's on composition-factor-groups. The following proof is much like Hölder's.

HÖLDER'S THEOREM.† *Two sets of composition-factor-groups of a given group G are identical except possibly in sequence.*

Suppose two composition-series developed from G which differ first in their $(i+1)$th terms:

$$G,\ H_1,\ \cdots,\ H_{i-1},\ H_i,\ \text{etc.};$$

and

$$G,\ H_1,\ \cdots,\ H_{i-1},\ H_i',\ \text{etc.}$$

Now C, the cross-cut of H_i and H_i', is invariant under H_{i-1} (p. 77, Ex. 8); hence we use it as head.

H_{i-1}	H_{i-1}/C
C	I

The subgroups of H_{i-1}/C corresponding to H_i and H_i' respectively, say S_i and S_i', by the theory of quotient groups

(a) are invariant and have only the identity in common;

(b) are maximum in H_{i-1}/C, because H_i and H_i' are maximum in H_{i-1}.

From (a), each element of S_i is commutative with each element of S_i' (§ 34, Th. 3, Cor.); and since S_i is a maximum invariant subgroup in H_{i-1}/C, the direct product of S_i and S_i' is H_{i-1}/C (p. 77, Ex. 6). Hence (*cf.* p. 82, Ex. 6).

(c)
$$\begin{cases} H_{i-1}/H_i = S_i', \text{ and} \\ H_{i-1}/H_i' = S_i. \end{cases}$$

(d) From (c), S_i and S_i' are simple, because H_i' and H_i are maximum in H_{i-1}.

* Jordan, *Traité des Substitutions* (1870), p. 42.

† Hölder, *Mathematische Annalen*, vol. XXXIV (1889), p. 37.

(*e*) From (*b*) and (*d*), C is a maximum invariant subgroup of H_i and of H_i'.

By assumption

$$(f) \qquad \begin{cases} H_i/C = S_i, \text{ and} \\ H_i'/C = S_i'. \end{cases}$$

The proof will now be completed by induction. The theorem is easily verified for groups of low composite orders, as 4 and 6. We assume it true for all groups of orders less than the order of G.

Since C is a maximum invariant subgroup in both H_i and H_i', it can be selected for the next term in either of the incomplete composition-series under discussion, giving

$$G,\ H_1,\ \cdots,\ H_{i-1},\ H_i,\ C;$$
$$G,\ H_1,\ \cdots,\ H_{i-1},\ H_i',\ C.$$

By (*c*) and (*f*) the corresponding composition-factor-groups would be

$$G/H_1,\ \cdots,\ S_i',\ S_i;$$
$$G/H_1,\ \cdots,\ S_i,\ S_i'.$$

As C is of lower order than is G, the assumption covers the terms from that point on, and the two composition-factor-groups of G are seen to be identical excepting as to arrangement.

Following directly from the preceding is

JORDAN'S THEOREM. *Two sets of composition-factors of a given group G are identical except possibly in sequence.*

55. Solvable and Insolvable Groups. A solvable group is one all of whose composition-factors are primes.* An insolvable group has at least one composition-factor that is

* A solvable group has sometimes been called *metacyclic*, although this term has been used also to designate a group of order $p(p-1)$ generated by s and t, where

$$s^p = t^{p-1} = I \text{ and } t^{-1}st = s^m,$$

m being a primitive root of the prime p.

composite. The composition-factors of the symmetric group of degree four are 2, 3, 2, 2, and it is thus solvable; those of the symmetric group of degree five are 2, 60 (*cf.* § 22, Th. 1) and it is thus insolvable.

From § 40 we see that every abelian group is solvable.

From § 45 every group of order p^m is solvable.

Solvable and insolvable groups derive their names from the theory of equations. In Chapter X it will be shown that to each algebraic equation there is, for a given number domain, a group, and that the equation can or cannot be solved (in that domain) by a finite number of the rational processes and root extractions according as the group is solvable or insolvable.

56. Other Series of Included Groups. There are several other series of included groups besides the ordinary composition-series. Thus, $G_0, G_1, G_2, \cdots, G_i, \cdots, G_n = I$, where each G_i is an invariant subgroup of G_0, is a **chief-series** of G_0 if G_i contains G_{i+1} but contains no invariant subgroup of G_0 containing G_{i+1}. The chief-series for the symmetric group of degree four would thus consist of the alternating group of degree four, the four-group, and the identity, because the four-group contains no invariant subgroup of the symmetric group excepting the identity.

By methods similar to those used in § 54 the following can be proved (G_0/G_1, G_1/G_2, etc., are called *chief-factor-groups* of G_0):

THEOREM. *Two sets of chief-factor-groups of a given group G are identical excepting possibly in sequence.*

The two series of included groups of the symmetric group of degree four used in § 53 and in this section illustrate the fact that if a chief-series, itself not an ordinary composition-

series, of a group is given, it is possible to form an ordinary composition-series by inserting some terms. That the reverse — obtaining a chief-series by omitting terms of an ordinary composition-series — is not always possible can be illustrated by using a four-group in the octic group.

Again, $G, C_1, C_2, \cdots, C_i, \cdots, C_n$ where each C is a characteristic subgroup of G, is a **characteristic-series** of G if C_i contains C_{i+1} but contains no characteristic subgroup of G containing C_{i+1}.

Finally, the successive groups may be obtained according to some law as in the series of derived groups in which each term is the commutator subgroup of the preceding term.

EXERCISES

1. Find the composition-series of the five groups of order 12. (*Cf.* § 46.)

2. Prove: The symmetric group of degree n is solvable, if and only if $n < 5$.

3. Discuss the solvability of groups of order pq where p and q are primes. (*Cf.* p. 118, Exercise 6; § 40, Theorem 3.)

4. Find a chief-series for a group G which is the direct product of the alternating group of degree four and the four-group.

5. Prove: Every perfect group is insolvable.

ADDITIONAL EXERCISES

1. Prove: A necessary condition that an element be invariant in the group of isomorphisms of an abelian group G is that it transform every element of G into the same power of itself. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), p. 102.

2. Prove: The symmetric group of degree $n > 2$, is complete excepting when $n = 6$. Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), § 65.

3. For a proof of the statement on page 112 that the group of isomorphisms of a cyclic group of order 2^n, $n > 2$, is an abelian group

of order 2^{n-1}, type $(n-2, 1)$, see Burnside, *Theory of Groups* (1911), p. 115, or Hilton, *Finite Groups* (1908), p. 138, Ex. 12.

4. A *Theorem of Young's.* If an automorphism of a group G exists in which every element corresponds to its αth power where α is prime to the order of G, then the $(\alpha - 1)$th power of every element of G is invariant. Young, J. W., *Transactions of the American Mathematical Society*, vol. 3 (1902), pp. 186, 187.

5. Prove: If a series of derived groups of a given group G leads to the identity, G is solvable; and conversely. Hilton, *Finite Groups* (1908), p. 166.

6. Prove: If the composition-factors of a solvable group G may be taken in any order, G is the direct product of prime-power groups. Burnside, *Theory of Groups* (1897), p. 131 or (1911), p. 75.

7. A *Theorem of Frobenius.* If the order of a group G is divisible by the square of no prime, G is solvable. *Cf.* Weber, H., *Lehrbuch der Algebra*, Zweiter Band (1899), § 36.

8. Prove the theorem of page 122.

CHAPTER IX

ON GROUPS OF LINEAR SUBSTITUTIONS

57. Introduction. The present Chapter aims only to mention a few things in Frobenius' theory of groups of linear substitutions. We shall employ x, y, z, etc., to represent variables and a, b, c, etc., to represent constants, variables and constants to be any real or ordinary complex numbers. Then, the following m linear homogeneous equations constitute a **linear substitution of degree m:**

$$\begin{array}{l} x_1 = a_{11}x_1' + a_{12}x_2' + \cdots + a_{1m}x_m', \\ x_2 = a_{21}x_1' + a_{22}x_2' + \cdots + a_{2m}x_m', \\ \cdots\cdots\cdots\cdots\cdots\cdots \\ x_m = a_{m1}x_1' + a_{m2}x_2' + \cdots + a_{mm}x_m'. \end{array} \qquad \begin{vmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \cdots & \cdots & \cdots & \cdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{vmatrix}$$

The determinant of the substitution (as shown at its right) may be denoted by $|a|$, and the corresponding matrix by $\|a\|$. Since each substitution which we use must have an inverse, $|a| \neq 0$, so that the system of equations can be solved for the x''s in terms of the x's.* Such a linear substitution is said to be *non-singular*.

Useful ways for indicating a linear substitution are easily shown by examples.

One form: $\begin{cases} x_1 = x_1' - x_2', \\ x_2 = x_1'. \end{cases}$

A two-line form: $\begin{pmatrix} x_1 & x_2 \\ x_1' - x_2' & x_1' \end{pmatrix}$,

* Bôcher, M., *Higher Algebra* (1907), § 16.

or dropping primes $\begin{pmatrix} x_1 & x_2 \\ x_1 - x_2 & x_1 \end{pmatrix}$.

Another form: $(x_1 - x_2, x_1)$.

We shall find it convenient to employ A, B, S, etc., for such substitutions; thus, $S \equiv (x_1 - x_2, x_1)$.

Multiplication will be explained with two linear substitutions of degree 3. Let

$$A \equiv (a_{11}x_1 + a_{12}x_2 + a_{13}x_3,\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3,\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3),$$
$$B \equiv (b_{11}x_1 + b_{12}x_2 + b_{13}x_3,\ b_{21}x_1 + b_{22}x_2 + b_{23}x_3,\ b_{31}x_1 + b_{32}x_2 + b_{33}x_3).$$

Then AB means A followed by B (or B substituted after A),* giving

$$\begin{aligned} AB \equiv (&(a_{11}b_{11} + a_{12}b_{21} + a_{13}b_{31})x_1 + (a_{11}b_{12} + a_{12}b_{22} + a_{13}b_{32})x_2 + (a_{11}b_{13} + a_{12}b_{23} + a_{13}b_{33})x_3,\\ &(a_{21}b_{11} + a_{22}b_{21} + a_{23}b_{31})x_1 + (a_{21}b_{12} + a_{22}b_{22} + a_{23}b_{32})x_2 + (a_{21}b_{13} + a_{22}b_{23} + a_{23}b_{33})x_3,\\ &(a_{31}b_{11} + a_{32}b_{21} + a_{33}b_{31})x_1 + (a_{31}b_{12} + a_{32}b_{22} + a_{33}b_{32})x_2 + (a_{31}b_{13} + a_{32}b_{23} + a_{33}b_{33})x_3), \end{aligned}$$

or $AB \equiv (c_{11}x_1 + c_{12}x_2 + c_{13}x_3,\ c_{21}x_1 + c_{22}x_2 + c_{23}x_3,\ c_{31}x_1 + c_{32}x_2 + c_{33}x_3)$

where $c_{ij} = a_{i1}b_{1j} + a_{i2}b_{2j} + a_{i3}b_{3j};\ i, j = 1, 2, 3.$

The student acquainted with the multiplication of determinants and matrices will know that $|a| \cdot |b| = |c|$ and $\|a\| \cdot \|b\| = \|c\|$, and will observe that accordingly the multiplication of linear substitutions of the same degree is associative but not in general commutative. Here, $\|a\|$, $\|b\|$, $\|c\|$ are respectively the matrices of the substitutions A, B, and C above.

The identical substitution of degree three is $I \equiv (x_1, x_2, x_3)$, and A^{-1}, the inverse of A, may be found by solving

$$\begin{aligned} x_1 &= a_{11}x_1' + a_{12}x_2' + a_{13}x_3', \\ x_2 &= a_{21}x_1' + a_{22}x_2' + a_{23}x_3', \\ x_3 &= a_{31}x_1' + a_{32}x_2' + a_{33}x_3', \end{aligned}$$

for x_1', x_2', and x_3'. Thus, for $S \equiv (x_1 - x_2, x_1)$, $S^{-1} \equiv (x_2, x_2 - x_1)$.

* Some writers reverse the process, using AB to mean A substituted after B.

The transform of $A \equiv (3x_1 - 4x_2 - 2x_3,\ 2x_1 - 3x_2 - 2x_3,\ x_2 + x_3)$ by $T \equiv (x_1 + x_2 + x_3,\ x_1 + x_2,\ -x_2 + x_3)$ is $T^{-1}AT$; and an easy and direct way for finding it is to use matrices, as follows:

$$\begin{Vmatrix} -1 & 2 & 1 \\ 1 & -1 & -1 \\ 1 & -1 & 0 \end{Vmatrix} \cdot \begin{Vmatrix} 3 & -4 & -2 \\ 2 & -3 & -2 \\ 0 & 1 & 1 \end{Vmatrix} \cdot \begin{Vmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 0 & -1 & 1 \end{Vmatrix} = \begin{Vmatrix} 0 & 1 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & 1 \end{Vmatrix} \cdot$$

Hence, $T^{-1}AT \equiv (x_2,\ -x_1,\ x_3)$.

If $S^m = I$ and m is the smallest positive, finite integer giving the identity, S is said to be of **period** m. There are many substitutions no finite power of which is the identity. But if

$$S \equiv (x_1 - x_2,\ x_1), \qquad S^4 \equiv (x_2 - x_1,\ -x_1),$$

then $S^2 \equiv (-x_2,\ x_1 - x_2), \quad S^5 \equiv (x_2,\ x_2 - x_1),$

$$S^3 \equiv (-x_1,\ -x_2), \qquad S^6 \equiv (x_1,\ x_2).$$

Hence, S is of period 6. (*Cf.* p. 73, Ex. 10.)

The **conjugate**, $\bar{A}$, of a linear substitution A is obtained from A by replacing a_{ij} by its (complex) conjugate $\bar{a}_{ij}$. Hence, A is real if $\bar{A} \equiv A$ (that is, if $a_{ij} = \bar{a}_{ij}$).

A linear substitution A is **symmetric** if $a_{ij} = a_{ji}$, and is **Hermitian** if $a_{ij} = \bar{a}_{ji}$.

The literal permutation introduced in Chapter II is obviously a special linear substitution in which each x is replaced by an x (a monomial) with coefficient $+1$.

58. The Linear Substitution Group. If A, B, C are linear substitutions of degree m, then $(AB)C = A(BC)$, because substituting B and A and then C in the result is the same as substituting C in B and then the result in A. Hence, if a finite set of non-singular linear substitutions is closed, the set forms a **linear substitution group.** (*Cf.* p. 7, Ex. 10.)

In a finite linear substitution group the determinant of any

substitution is a root of unity. Because any substitution A must be of finite period, say n, then, since $A^n = I$, $|\ a\ |^n$ must equal the determinant of the identical substitution, or 1.

If each constant and variable of a given substitution is replaced by its conjugate imaginary, we obtain a group $\bar{G}$ simply isomorphic with G. Each of these two groups is known as the **conjugate-imaginary** of the other.

EXERCISES

1. Determine whether

$$S \equiv (x_1 + x_2 + x_3, \quad x_1 + 2x_2 + x_3, \quad 3x_1 - x_2 + x_3)$$

and $T \equiv (x_1 + x_2 + x_3, \quad x_1 + x_3, \quad x_1 + x_2 + x_3)$ are commutative.

2. Write the cyclic group generated by $\left(\dfrac{x-y}{\sqrt{2}}, \quad \dfrac{x+y}{\sqrt{2}}\right)$.

3. Find the condition that $(x \cos\theta - y \sin\theta,\ x \sin\theta + y \cos\theta)$ be of finite period n.

4. Find the nth power of $S \equiv (ax + by,\ cy)$, and therefrom the conditions that S be of period n.

5. If $S \equiv (2x_1 + x_2,\ x_1 - 3x_2)$ and $T \equiv (3x_1 - x_2,\ 5x_1 - 2x_2)$, find T^{-1} and show that $(T^{-1}S)T = T^{-1}(ST)$.

6. In the preceding Exercise the substitution S was transformed by T. Now find out into what T transforms each of the linear functions $2x_1 + x_2$ and $x_1 - 3x_2$. How can this be done by matrices?

7. $S \equiv (-x_2, x_1)$ and $T \equiv (x_1, -x_2)$ generate a group of order eight. Write all the elements and name the group (abstractly).

Exercises 8–11 following are not about linear homogeneous substitutions, but as the methods just used are applicable, the exercises are not irrelevant. They have to do with the *linear fractional substitution* $y = \dfrac{ax+b}{cx+d}$, in which we assume $c \neq 0$ (Why?) and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. (Why?)

8. Write the substitutions of the cyclic group generated by the substitution $\dfrac{3x-7}{x-2}$.

9. Prove that $a + d = 0$ is a condition that $y = \dfrac{ax + b}{cx + d}$ be a substitution of period 2. Hint. Substitute y in $z = \dfrac{ay + b}{cy + d}$, then use the identity $z = x$.

10. Find a necessary and sufficient condition that $\dfrac{ax + b}{cx + d}$ be a substitution of period 3. Ans. $a^2 + ad + bc + d^2 = 0$.

11. Show that $\dfrac{cx^2 + b}{cx - a}$ is an invariant of the substitution $\dfrac{ax + b}{cx - a}$.

59. Hermitians. A Hermitian linear substitution has been defined previously (§ 57). The following quadratic polynomial in 2 m variables, x_i and y_j; $i, j = 1, \cdots, m$,

$$\begin{aligned} &a_{11}x_1y_1 + a_{12}x_1y_2 + \cdots + a_{1m}\ x_1y_m \\ &+ a_{21}x_2y_1 + a_{22}x_2y_2 + \cdots + a_{2m}x_2y_m \\ &+ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &+ a_{m1}x_my_1 + a_{m2}x_my_2 + \cdots + a_{mm}x_my_m \end{aligned}$$

is called a **bilinear form**, and may be represented by $\sum_1^m a_{ij}x_iy_j$.

A **Hermitian form** is a bilinear form $\Sigma\, a_{ij}x_i\bar{x}_j$, in which $a_{ij} = \bar{a}_{ji}$ (*i.e.*, the conjugate of a_{ji}), $\bar{x}_j$ is the conjugate of x_j, and $i, j = 1, 2, \cdots, m$. (a_{ii} is real.)

A Hermitian form is said to be **positive-definite** if it is positive for all values of its variables excepting for $x_1 = x_2 = \cdots = x_m = 0$.

THEOREM 1. *If the variables of the Hermitian form* $\sum_1^m a_{ij}x_i\bar{x}_j$ $(i, j = 1, \cdots, m)$, *are replaced by the substitutions*

$$x_1 = c_{11}y_1 + c_{12}y_2 + \cdots + c_{1m}y_m, \quad \bar{x}_1 = \bar{c}_{11}\bar{y}_1 + \bar{c}_{12}\bar{y}_2 + \cdots + \bar{c}_{1m}\bar{y}_m,$$
$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \qquad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$
$$x_m = c_{m1}y_1 + c_{m2}y_2 + \cdots + c_{mm}y_m, \quad \bar{x}_m = \bar{c}_{m1}\bar{y}_1 + \bar{c}_{m2}\bar{y}_2 + \cdots + \bar{c}_{mm}\bar{y}_m,$$

the new form is Hermitian.

We give a proof for $m = 2$. The steps for $m > 2$ may be made analogously, *mutatis mutandis*. In the following given Hermitian form notice that a_{11} and a_{22} are their own conjugates (and hence real):

$$a_{11}x_1\bar{x}_1 + a_{12}x_1\bar{x}_2 + \bar{a}_{12}x_2\bar{x}_1 + a_{22}x_2\bar{x}_2.$$

Substitutions:

$$x_1 = c_{11}y_1 + c_{12}y_2, \qquad \bar{x}_1 = \bar{c}_{11}\bar{y}_1 + \bar{c}_{12}\bar{y}_2,$$
$$x_2 = c_{21}y_1 + c_{22}y_2; \qquad \bar{x}_2 = \bar{c}_{21}\bar{y}_1 + \bar{c}_{22}\bar{y}_2.$$

The new form is

$$\begin{aligned}&(a_{11}c_{11}\bar{c}_{11} + a_{12}c_{11}\bar{c}_{21} + \bar{a}_{12}c_{21}\bar{c}_{11} + a_{22}c_{21}\bar{c}_{21})y_1\bar{y}_1 \\ &\qquad + (a_{11}c_{11}\bar{c}_{12} + a_{12}c_{11}\bar{c}_{22} + \bar{a}_{12}c_{21}\bar{c}_{12} + a_{22}c_{21}\bar{c}_{22})y_1\bar{y}_2 \\ &+ (a_{11}c_{12}\bar{c}_{11} + a_{12}c_{12}\bar{c}_{21} + \bar{a}_{12}c_{22}\bar{c}_{11} + a_{22}c_{22}\bar{c}_{21})y_2\bar{y}_1 \\ &\qquad + (a_{11}c_{12}\bar{c}_{12} + a_{12}c_{12}\bar{c}_{22} + \bar{a}_{12}c_{22}\bar{c}_{12} + a_{22}c_{22}\bar{c}_{22})y_2\bar{y}_2.\end{aligned}$$

Remembering that the sum or the product of two complex conjugates is real, and that such pairs as $\bar{a}_{12}c_{22}\bar{c}_{11}$ and $a_{12}c_{11}\bar{c}_{22}$ are conjugates, we see that the new form is Hermitian.

The student familiar with the theory of matrices will appreciate the following proof of this theorem. From the definition given for a Hermitian form we may say that a necessary and sufficient condition that the linear form $\Sigma a_{ij}x_i\bar{x}_j$, in which $\bar{x}_j$ is the conjugate imaginary of x_j, be Hermitian is that the matrix of the coefficients be identically equal to the matrix formed by interchanging a_{ij} and a_{ji} in its conjugate ($i, j = 1, \cdots, m$).

Subjecting the variables of the given Hermitian form to the given linear substitutions gives (in factor form) for the matrix of the resulting bilinear form*

* Bôcher, M., *Higher Algebra* (1907), p. 115. **Note that Bôcher uses "conjugate" to indicate interchanging a_{ij} and a_{ji}.**

$$\begin{Vmatrix} c_{11} & c_{21} & \cdots & c_{m1} \\ c_{12} & c_{22} & \cdots & c_{m2} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ c_{1m} & c_{2m} & \cdots & c_{mm} \end{Vmatrix} \cdot \begin{Vmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ \bar{a}_{12} & a_{22} & \cdots & a_{2m} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \bar{a}_{1m} & \bar{a}_{2m} & \cdots & a_{mm} \end{Vmatrix} \cdot \begin{Vmatrix} \bar{c}_{11} & \bar{c}_{12} & \cdots & \bar{c}_{1m} \\ \bar{c}_{21} & \bar{c}_{22} & \cdots & \bar{c}_{2m} \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ \bar{c}_{m1} & \bar{c}_{m2} & \cdots & \bar{c}_{mm} \end{Vmatrix} \cdot \quad (1)$$

To show that this is Hermitian, we form the conjugate by replacing each element by its complex imaginary,

$$\begin{Vmatrix} \bar{c}_{11} & \cdot & \cdot & \cdot & \bar{c}_{m1} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \bar{c}_{1m} & \cdot & \cdot & \cdot & \bar{c}_{mm} \end{Vmatrix} \cdot \begin{Vmatrix} a_{11} & \cdot & \cdot & \cdot & \bar{a}_{1m} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ a_{1m} & \cdot & \cdot & \cdot & a_{mm} \end{Vmatrix} \cdot \begin{Vmatrix} c_{11} & \cdot & \cdot & \cdot & c_{1m} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ c_{m1} & \cdot & \cdot & \cdot & c_{mm} \end{Vmatrix};$$

and then interchange a_{ij} and a_{ji}, which is affected for a product of matrices by making the interchange in each factor and reversing the order of the factors.* The following then results, and since it is identically equal to (1), the corresponding linear form is Hermitian:

$$\begin{Vmatrix} c_{11} & \cdot & \cdot & \cdot & c_{m1} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ c_{1m} & \cdot & \cdot & \cdot & c_{mm} \end{Vmatrix} \cdot \begin{Vmatrix} a_{11} & \cdot & \cdot & \cdot & a_{1m} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \bar{a}_{1m} & \cdot & \cdot & \cdot & a_{mm} \end{Vmatrix} \cdot \begin{Vmatrix} \bar{c}_{11} & \cdot & \cdot & \cdot & \bar{c}_{1m} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ \bar{c}_{m1} & \cdot & \cdot & \cdot & \bar{c}_{mm} \end{Vmatrix} \cdot$$

We shall next state without proof an interesting theorem, *viz.*,

THEOREM 2. *By suitably chosen linear substitutions any positive-definite Hermitian form in m variables can be changed to* $y_1\bar{y}_1 + y_2\bar{y}_2 + \cdots + y_m\bar{y}_m$.

For reference to a proof see Additional Exercise 1 at the end of this Chapter.

* *L.c.*, p. 65.

60. Absolute and Relative Invariants. If every element of a substitution group G (linear or otherwise) on the variables $x_1, \cdots, x_m$ transforms the function $f(x_1, \cdots, x_m)$ into itself (formally) multiplied by a constant not zero, the function is said to be *invariant under the group.* The function is an **absolute invariant** (frequently called simply "invariant") if the constant is unity, a **relative invariant** if the constant is not unity. In § 5 we had an example of an absolute invariant under a group. Under the group generated by $(-x_2, x_1)$ the binomial $x_1^2 - x_2^2$ is a relative invariant.

THEOREM 1. *Any finite substitution group G (linear or otherwise) has invariants.*

For if G is of degree m, its elements can change $f_1(x_1, \cdots, x_m)$ into but a finite set of functions, $f_1, f_2, \cdots, f_n$. Any symmetric function (as sum, product, etc.) of all the f's evidently is invariant under G.

THEOREM. 2. LOEWY'S THEOREM.* *For any pair of conjugate imaginary finite linear substitution groups, G and $\bar{G}$, there is at least one positive-definite Hermitian form which is invariant when its conjugate variables are subjected to corresponding elements of G and $\bar{G}$.*

For, if G is of degree m on $x_1, \cdots, x_m$ and $\bar{G}$ on $\bar{x}_1, \cdots, \bar{x}_m$, and each pair of corresponding elements changes the positive-definite form $J_1(x_1, \cdots, x_m, \bar{x}_1, \cdots, \bar{x}_m)$ into the set $J_1, J_2, \cdots, J_n$, then each J is a positive-definite form (§ 59). Accordingly, $J_1 + J_2 + \cdots + J_n$ is a positive-definite Hermitian form which is invariant under each pair of corresponding elements of G and $\bar{G}$.

EXAMPLE. The following matrices represent the substitu-

* *Comptes Rendus*, vol. 123 (1896), p. 168.

tions of the non-cyclic group G of order 6 (ω is an imaginary cube-root of unity).

$$\left\|\begin{matrix}1&0&0\\0&1&0\\0&0&1\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&\omega&0\\0&0&\omega^2\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&\omega^2&0\\0&0&\omega\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&0&1\\0&1&0\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&0&\omega^2\\0&\omega&0\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&0&\omega\\0&\omega^2&0\end{matrix}\right\|.$$

The conjugate group $\bar{G}$ is

$$\left\|\begin{matrix}1&0&0\\0&1&0\\0&0&1\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&\omega^2&0\\0&0&\omega\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&\omega&0\\0&0&\omega^2\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&0&1\\0&1&0\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&0&\omega\\0&\omega^2&0\end{matrix}\right\|,\ \left\|\begin{matrix}1&0&0\\0&0&\omega^2\\0&\omega&0\end{matrix}\right\|.$$

These groups transform $J = x_1\bar{x}_1$ into itself, so $x_1\bar{x}_1$ is an invariant positive-definite Hermitian form under them. But the groups transform $J_1 = x_2\bar{x}_2$ into itself and into $J_2 = x_3\bar{x}_3$. Hence $x_2\bar{x}_2 + x_3\bar{x}_3$ is another invariant positive-definite Hermitian form under these groups.

EXERCISES

1. Show that $x_1 - x_2 + x_3$ is invariant under the group generated by $(-3\,x_1 + 3\,x_2 - 4\,x_3, -x_2, 2\,x_1 - 3\,x_2 + 3\,x_3)$ and $(x_1 + x_3, 2\,x_1 + x_3, x_2 - x_3)$. Is it a relative or an absolute invariant?

2. Prove: If the determinant of the generating element of a cyclic linear substitution group G is symmetric, the determinant of each element of G is symmetric.

3. (*a*) Write the group G generated by $S \equiv (ix_1, -x_2)$ and write the conjugate-imaginary group $\bar{G}$. ($i = \sqrt{-1}$.)

(*b*) Find a positive-definite Hermitian form invariant under the groups G and $\bar{G}$ of part (*a*).

4. Find a positive-definite Hermitian form invariant under the group G generated by $S \equiv (-x_2, x_1)$ and $T \equiv (x_1, -x_2)$, and its conjugate $\bar{G}$. *Cf.* p. 128, Ex. 7.

61. Characteristic Equation of a Linear Substitution. We shall explain what the characteristic equation of a linear substitution is, in the proof of the following theorem.

THEOREM 1. *For any non-singular linear substitution A on*

the m variables $x_1, \cdots, x_m$ *there is at least one relative (or absolute) invariant of the form* $l_1x_1 + \cdots + l_mx_m$, *where not all the l's are zeros.*

If $A \equiv (a_{11}x_1 + \cdots + a_{1m}x_m, \cdots, a_{m1}x_1 + \cdots + a_{mm}x_m)$, we have to show that unknown constants, $l_1, \cdots, l_m$, can be found such that

$$l_1(a_{11}x_1 + \cdots + a_{1m}x_m) + \cdots + l_m(a_{m1}x_1 + \cdots + a_{mm}x_m) \equiv \theta \cdot (l_1x_1 + \cdots + l_mx_m),$$

where θ is a constant not zero. This gives rise to a system of m linear homogeneous equations:

$$\begin{aligned}
(a_{11} - \theta)l_1 + \quad & a_{21}l_2 + \cdots + \quad a_{m1}l_m = 0, \\
a_{12}l_1 + (a_{22} - \theta)l_2 + \cdots + \quad & a_{m2}l_m = 0, \\
\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad & \cdot \quad \cdot \quad \cdot \\
a_{1m}l_1 + \quad & a_{2m}l_2 + \cdots + (a_{mm} - \theta)l_m = 0.
\end{aligned}$$

A necessary and sufficient condition that this system have a solution other than $l_1 = l_2 = \cdots = l_m = 0$ is that the determinant

$$\begin{vmatrix}
a_{11} - \theta & a_{21} & \cdots & a_{m1} \\
a_{12} & a_{22} - \theta & \cdots & a_{m2} \\
\cdot & \cdot & \cdot & \cdot \\
a_{1m} & a_{2m} & \cdots & a_{mm} - \theta
\end{vmatrix} = 0.^*$$

This mth degree equation in θ is known as the **characteristic equation** of the linear substitution A. Note how this equation can be written in determinant form directly from the linear substitution A. Its constant term is $|a|$, which by hypothesis $\neq 0$. Hence, a non-zero value of θ exists and A has at least one linear invariant. Substitution A can have no linear invariants other than those corresponding to the roots of its characteristic equation. If one root of the characteristic equation is $\theta = 1$, A has an absolute invariant.

62. Lemmas on Invariants. LEMMA 1. *If a function*

* *Cf.* Bôcher, M., *Higher Algebra* (1907), p. 47.

$\Phi(x_1, \cdots, x_m)$ is invariant (absolute or relative) under a linear substitution group G on the variables $x_1, \cdots, x_m$, then $\Phi(f_1, f_2, \cdots, f_m)$ is an invariant of the group $T^{-1}GT$, where T is the non-singular linear substitution $x_i = f_i(y_1, \cdots, y_m)$, $i = 1, \cdots, m$.

This proposition needs no formal proof. We may illustrate it by using $C \equiv (2x_2 - x_1, x_2)$ and $D \equiv (x_2, 2x_2 - x_1)$. $(x_1 - x_2)^2$ is seen to be invariant under the group generated by C and D. Transforming by $x_1 = y_1 + y_2$, $x_2 = y_2$ changes the invariant to y_1^2, which is invariant under the transformed group generated by $C' \equiv (-y_1, y_2)$ and $D' \equiv (y_1, y_2 - y_1)$.

As extensions or corollaries of the preceding observation we have

LEMMA 2. *If n functions $\Phi_j(x_1, \cdots, x_m)$, $j = 1, \cdots, n$, are transformed only among themselves by the elements of a linear substitution group G on the variables $x_1, \cdots, x_m$, then $\Phi_j(f_1, f_2, \cdots, f_m)$, $j = 1, \cdots, n$, are transformed only among themselves by the group $T^{-1}GT$, where T is the non-singular linear substitution $x_i = f_i(y_1, \cdots, y_m)$, $i = 1, \cdots, m$.*

LEMMA 3. *If n functions $\Phi_j(x_1, \cdots, x_m)$, $j = 1, \cdots, n$, are transformed into functions of themselves alone by the elements of a linear substitution group on the variables $x_1, \cdots, x_m$, then $\Phi_j(f_1, \cdots, f_m)$, $j = 1, \cdots, n$, are transformed only into functions of themselves by the group $T^{-1}GT$, where T is the non-singular linear substitution $x_i = f_i(y_1, \cdots, y_m)$, $i = 1, \cdots, m$.*

From Lemma 1 we see that if a linear substitution S on the m variables $x_1, \cdots, x_m$ transforms $l_1x_1 + \cdots + l_mx_m$ (where not all the l's are zeros) into $\theta \cdot (l_1x_1 + \cdots + l_mx_m)$, then $T^{-1}ST$ transforms $l_1f_1 + \cdots + l_mf_m$ into $\theta \cdot (l_1f_1 + \cdots + l_mf_m)$ where T is the linear substitution $x_i = f_i(y_1, \cdots, y_m)$, $i = 1, \cdots, m$. Hence, if θ is a root of the characteristic equation of S, it is a root of the characteristic equation of $T^{-1}ST$, and conversely, or

THEOREM. *The roots of the characteristic equation of the transform of a linear substitution S are the same as the roots of the characteristic equation of S.* (*S and its transform are non-singular.*)

63. Reducible and Irreducible Linear Substitution Groups. The set of variables x_1, x_2 is seen to be invariant under $A \equiv (x_2, -x_1, x_1 - x_3)$ and $B \equiv (x_1, x_1 - x_2, x_3)$. Hence the linear substitution group generated by A and B is called a reducible group. In general, a linear substitution group G on m variables $x_1, \cdots, x_m$ is said to be **reducible** if some n $(0 < n < m)$ of the variables are taken over by each substitution of G into linear functions involving none of the other $m-n$ variables, or if G can by a linear substitution be transformed into a group on new variables for which such a property holds. A linear substitution group for which such a property is wanting is said to be **irreducible.**

If every element of the reducible group G on the m variables $x_1, \cdots, x_m$ takes over $x_1, \cdots, x_n$, where $0 < n < m$, into linear functions of themselves only, the determinant of each element is of the form

$$\begin{vmatrix} a_{11} \cdots a_{1n} & 0 \cdots 0 \\ \cdot \quad\quad \cdot & \cdot \quad \cdot \\ \cdot \quad\quad \cdot & \cdot \quad \cdot \\ a_{n1} \cdots a_{nn} & 0 \cdots 0 \\ a_{n+1\,1} & \cdots\cdots\; a_{n+1\,m} \\ \cdot & \quad\quad\quad\; \cdot \\ \cdot & \quad\quad\quad\; \cdot \\ a_{m1} & \cdots\cdots\cdots\; a_{mm} \end{vmatrix} .$$

EXAMPLE. The group G generated by $C \equiv (2x_2 - x_1, x_2)$ and $D \equiv (x_2, 2x_2 - x_1)$ does not appear to be reducible; but if these

generators are transformed by $x_1 = y_1 + y_2$, $x_2 = y_2$, we obtain $C' \equiv (-y_1, y_2)$ and $D' \equiv (y_1, y_2 - y_1)$. C' and D' generate a group G' whose elements change y_1 into functions not containing y_2. Hence, both G' and G are reducible.

THEOREM 1. *A necessary and sufficient condition that a linear substitution group G on the variables $x_1, \cdots, x_m (m > 1)$ be reducible is that there exist n, $0 < n < m$, linearly independent linear functions $l_{i1}x_1 + \cdots + l_{in}x_n$, $i = 1, \cdots, n$, which are transformed into linear functions of themselves alone by each substitution of G.**

SUFFICIENCY. We may assume the variables so arranged that

$$\begin{vmatrix} l_{11} \cdots l_{1n} \\ \cdot \quad \cdot \\ \cdot \quad \cdot \\ l_{n1} \cdots l_{nn} \end{vmatrix} \neq 0,$$

and then form the substitution S following, whose determinant is seen not to be zero:

$$\begin{aligned} y_1 &= l_{11}x_1 + \cdots + l_{1n}x_n, \\ &\cdot \quad \cdot \quad \cdot \\ y_n &= l_{n1}x_1 + \cdots + l_{nn}x_n, \\ y_{n+1} &= x_{n+1}, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \\ y_m &= x_m. \end{aligned}$$

If G is transformed by S, a new group G' is obtained. By Lemma 3 of § 62 it is seen that $y_1, y_2, \cdots, y_n$ go over into linear

* *Cf.* Reducible groups as defined in Burnside, W., *Finite Groups* (1911), p. 258; Manning, W. A., *Primitive Groups*, Part I (1921), p. 54.

functions of themselves alone by every element of G'. Hence G' is reducible, and therefore so also is G.

NECESSITY. If the determinant of every element of G is of the form

$$\begin{vmatrix} a_{11} & a_{1n} & 0 & \cdots & 0 \\ \cdot & \cdot & \cdot & & \cdot \\ \cdot & \cdot & \cdot & & \cdot \\ a_{n1} & a_{nn} & 0 & \cdots & 0 \\ a_{n+11} & \cdots & \cdots & & a_{n+1\,m} \\ \cdot & & & & \cdot \\ \cdot & & & & \cdot \\ a_{m1} & \cdots & \cdots & & a_{mm} \end{vmatrix},$$

evidently $x_1, \cdots, x_n$ are a set of linearly independent functions which are transformed into linear functions of themselves alone by each element of G.

If G is reducible and the determinant of any element fails to be of the form just employed, we can transform G into H by a linear substitution T, $x_i = f_i(y_1, \cdots, y_m)$, $i = 1, \cdots, m$, such that $y_1, \cdots, y_n$, $0 < n < m$, are taken over by each element of H into linear functions of themselves alone. Then from Lemma 3 of § 62, the linear functions of the n x's into which T^{-1} changes $y_1, \cdots, y_n$ would be transformed into linear functions of themselves alone by each element of G.

A **completely reducible** linear substitution group is one that has the following property or that can be transformed into one having this property: its m variables $x_1, \cdots, x_m$ can be separated into two or more sets such (*i*) that every element of the group takes each variable of any given set over into linear functions of the variables of that set alone, and (*ii*) that the group is irreducible when considered as affecting the variables

of any one set (that is, each set is irreducible). The determinant of each substitution is thus of the form

$$\begin{vmatrix} D_1 & & & \\ & D_2 & & \\ & & \cdot & \\ & & & \cdot \end{vmatrix}$$

where the D's are non-zero determinants with their principal diagonals along the principal diagonal, and all elements outside the D's are zeros.

EXAMPLE. If the generators

$$A \equiv (3x_1 - 4x_2 - 2x_3,\ 2x_1 - 3x_2 - 2x_3,\ x_2 + x_3)$$

and $$B \equiv (-3x_1 + 4x_2 + 2x_3,\ -2x_1 + 3x_2 + 2x_3,\ -x_3)$$

of the group G are transformed by

$$T \equiv (y_1 + y_2 + y_3,\ y_1 + y_2,\ -y_2 + y_3),$$

we obtain $A' \equiv T^{-1}AT \equiv (y_2,\ -y_1,\ y_3)$, (*cf.* § 57)

and $B' \equiv T^{-1}BT \equiv (y_1,\ -y_2\ ,-y_3)$, which generate G'. In A' and B', y_1 and y_2 are taken over into linear functions of themselves alone, and y_3 into linear functions of itself; also $(y_2,\ -y_1)$ and $(y_1,\ -y_2)$ generate an irreducible group (see Ex. 4 following this section). Hence, G' and G are completely reducible.

We close this section with an interesting theorem (from Frobenius*) which we shall leave unproved. (See, however, p. 140, Additional Ex. 4.)

THEOREM 2. *If a finite linear substitution group is reducible, it is completely reducible.*

* *Berliner Sitzungsberichte* (1896).

EXERCISES

1. In the characteristic equation of a linear substitution A, show (*i*) that the determinant, $|\ a\ |$, is the product of the roots, and (*ii*) that the sum of the roots is $a_{11} + a_{22} + \cdots + a_{mm}$.

2. The sum $a_{11} + a_{22} + \cdots + a_{mm}$ is called the **characteristic** of the linear substitution A. Prove: The characteristic (as well as the value of the determinant) of a linear substitution A is invariant in value under a non-singular transformation on the same variables.

3. If ω is an imaginary cube root of unity, $(y,\ x)$ and $(\omega^2 y,\ \omega x)$ generate a group of order 6. Find an invariant under this group.

4. Show that the group generated by $(x_2, -x_1)$ and $(x_1, -x_2)$ is irreducible.

5. By use of the characteristic equation of $S \equiv (x + y, -y, z - y)$ determine one or more linear invariants under the group generated by S.

6. Show that the group generated by S in the preceding exercise is completely reducible.

ADDITIONAL EXERCISES

1. Prove Theorem 2 in § 59. *Cf.* Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), § 91; or Manning, W. A., *Primitive Groups*, Part I (1921), § 26.

2. Professor Burnside shows that the group of isomorphisms of an abelian group of order p^n, type (1, 1, etc.) is a linear homogeneous congruence group. Burnside, *Theory of Groups* (1897), § 171; or (1911), § 89.

3. Let the substitution A' be formed from A by interchanging a_{ij} and a_{ji} (for all values of i and j). Definition. A is an **orthogonal substitution** if $AA' = I$. Prove that if A is orthogonal, $x_1^2 + x_2^2 + \cdots + x_m^2$ is invariant under it, and conversely. *Cf.* Hilton, H., *Finite Groups* (1908), p. 16.

4. For a proof of Theorem 2 of § 63 see Hilton, H., *Finite Groups* (1908), Chapter VII, § 7.

CHAPTER X

SOME APPLICATIONS OF GROUP THEORY IN OTHER FIELDS

64. Topics in this Chapter. We have already studied some groups in connection with the theory of numbers, matrices, and movements of geometrical magnitudes. Here will be presented, first, an outline of the Lagrange-Galois theory of algebraic equations, then, a few words on Lie's one-parameter groups in differential equations. The former develops a criterion of solvability of an algebraic equation. We shall attempt to build up the theory by means of theorems, but shall omit the proofs of some of them.* A few number theory concepts are explained, but it is assumed that the student is familiar with some of the classical theory of the algebraic equation. Some of the Galois theory is applied to two classical problems in construction by ruler and compasses. The part on Lie's one-parameter groups will mean little to one who has not had a first course in differential equations.

AN OUTLINE OF THE LAGRANGE-GALOIS THEORY

65. Preliminary Ideas. In the equation $x^n - c_1 x^{n-1} + \cdots + (-1)^n c_n = 0$ the c's are (constants or variables) assumed to be real or complex numbers and are known to equal the *elementary symmetric functions* of the n roots of the equation.

The rational operations of arithmetic and algebra are addi-

* The author constructs his outline from Professor L. E. Dickson's *Theory of Algebraic Equations* (1903) and from his Part III of Miller, Blichfeldt, and Dickson's *Finite Groups* (1916). *Cf.* Edgar Dehn's monograph, *Algebraic Equations* (1930).

tion, subtraction, multiplication, and division (by a number not zero).

A **number domain** * consists of all the numbers formed from a set of numbers (real or imaginary), $k_1, k_2, \cdots, k_m$, by a finite number of rational operations. It may be denoted by $R(k_1, \cdots, k_m)$. Evidently the set of all rational numbers forms the rational domain, which is indicated by $R(1)$, and furthermore $R(1)$ is contained in every domain.

Any number which is a root of an algebraic equation $x^n - c_1x^{n-1} + \cdots + (-1)^n c_n = 0$, whose coefficients are rational numbers, is an **algebraic number.** †

FUNDAMENTAL THEOREM OF SYMMETRIC FUNCTIONS. *Every rational symmetrical function of the roots $x_1, \cdots, x_n$ can be expressed as a rational function of the coefficients $c_1, \cdots, c_n$.*

If all the coefficients of the polynomial $f(x) \equiv a_0x^n + a_1x^{n-1} + \cdots + a_n$ belong to an algebraic number domain R, $f(x)$ is said to be a **rational integral function in domain** R, and $f(x) = 0$ an **equation in domain** R. If $n > 1$ and if $f(x)$ equals the product of two or more rational integral functions each in domain R and each of degree $< n$, $f(x)$ is **reducible in** R; otherwise, it is **irreducible in** R. The algebraic equation $f(x) = 0$ is said to be **reducible in** R, if $f(x)$ is reducible in R; otherwise it is an equation **irreducible in** R.

66. Preliminary Theory. THEOREM A. *If $x_1, \cdots, x_n$ are the (distinct* ‡*) roots of the numerical equation $f(x) \equiv x^n - c_1x^{n-1}$*

* Called also *realm*, *körper*, *field*, etc.

† If a number is a root of no such algebraic equation, it is called a *transcendental* number. In 1873 Hermite first proved e to be transcendental and in 1882 Lindemann that π is transcendental.

‡ If $f(x) = 0$ has multiple roots, use the Euclidean algorithm to find $g(x)$, the g.c.d. of $f(x)$ and $f'(x)$. Then proceed with $f(x)/g(x) = 0$, an equation which is in domain R and which has all the distinct roots of $f(x) = 0$ as simple roots and has no other roots.

$+ \cdots + (-1)^n c_n = 0$ *in the domain* R, *integers* $m_1, m_2, \cdots, m_n$ *can be found such that* $m_1x_1 + m_2x_2 + \cdots + m_nx_n$ *gives* $n!$ *distinct values (no two numerically equal) under the permutations of the symmetric group on* $x_1, \cdots, x_n$.

For a proof see Exercise 8 of p. 147.

Let $V_1 = m_1x_1 + m_2x_2 + \cdots + m_nx_n$ (sometimes called the **Galois function**), let $s_1(= I), s_2, \cdots, s_{n!}$ be the permutations of the symmetric group on $x_1, \cdots, x_n$, and let $V_1, V_2, \cdots, V_{n!}$ be the (distinct) polynomials formed when the s's are applied to V_1. Since any s merely permutes the V's among themselves, any symmetric function of the V's is invariant under every s and therefore is symmetric in the x's (§ 9). Accordingly, by the Fundamental Theorem in § 65 the equation $F(y) \equiv (y - V_1)(y - V_2) \cdots (y - V_{n!}) = 0$ is in the domain R. If $G(y)$ is that factor of $F(y)$ such that $G(y)$ is irreducible in R and $G(V_1) = 0$, then $G(y) = 0$ is called **a Galois resolvent** of the given equation $f(x) = 0$.

LEMMA 1. *Given that the algebraic equations* $\phi(x) = 0$ *and* $\psi(x) = 0$ *are in the domain* R, *and that* $\phi(x) = 0$ *is irreducible in* R. *Then if one root of* $\phi(x) = 0$ *satisfies* $\psi(x) = 0$, *every root of* $\phi(x) = 0$ *satisfies* $\psi(x) = 0$.

Using the Euclidean algorithm to find the greatest common divisor, $g(x)$, of $\phi(x)$ and $\psi(x)$ involves only the rational operations; hence, $g(x)$ is in the domain R. From the hypothesis, the degree of $g(x)$ is > 0. It is easy to see that if the degree of $g(x)$ is less than the degree of $\phi(x)$, then $\phi(x)$ is reducible in R. But this is contrary to hypothesis, and hence every root of $\phi(x) = 0$ satisfies $g(x) = 0$ and thus satisfies $\psi(x) = 0$.

The next proposition is one which Abel stated but did not prove. The proof here is due to Galois.

LEMMA 2. *Any root of the given equation* $f(x) \equiv x^n - c_1x^{n-1} + \cdots + (-1)^n c_n = 0$ *of domain* R *can be expressed as a rational function of the Galois function* V_1, *with coefficients in* R.

It will be shown how x_1 can be so expressed. Corresponding to the symmetric group on $x_2, \cdots, x_n$ we have $(n-1)! = k$ distinct values of V_1, *viz.*, $V_1, \cdots, V_k$. The coefficients of the equation $K(z) \equiv (z - V_1)(z - V_2) \cdots (z - V_k) = 0$ are integral symmetric functions of the k V's, hence we express them as integral functions (with integral coefficients) of the coefficients of $f(x)/(x-x_1) = 0$ and of powers of x_1. Now each coefficient of $f(x)/(x-x_1) = 0$ is a polynomial in the coefficients of $f(x) = 0$ and powers of x_1, hence we may write the z-equation as an equation in both z and x_1, say $K(z, x_1) = 0$. Since $K(V_1, x_1) \equiv 0$, the equation $K(V_1, x) = 0$ has the root x_1 in common with the equation $f(x) = 0$. These two equations have no other root in common.* Using the Euclidean algorithm to find the g.c.d. of $f(x)$ and $K(V_1, x)$ gives ultimately a remainder of the first degree in x. As this must equal zero, we obtain immediately a rational function for x_1 in terms of V_1 and with coefficients in R.

As an immediate corollary of the preceding we have

LEMMA 3. *Any root of the Galois resolvent equation can be expressed as a rational function with coefficients in* R, *of the Galois function* V_1.

THEOREM B AND DEFINITION. *If* $G(y) = 0$ *is the Galois resolvent of the equation* $f(x) = 0$, *then the permutations on* $x_1, \cdots, x_n$ *that transform the Galois function* V_1 *into all the roots of*

* For another root, as x_2, of $f(x) = 0$ will not satisfy $K(V_1, x) = 0$. To show that $K(V_1, x_2) \neq 0$ we may substitute in $K(z)$ as follows: in each of the k V's substitute x_2 for x_1, and then for z substitute V_1. As no one of the k factors vanishes, $K(V_1, x_2) \neq 0$.

$G(y) = 0$ *form a group, which is called the* **group of the given equation** $f(x) = 0$ *for the domain* R.

PROOF. If s and t, distinct permutations on $x_1, \cdots, x_n$, transform V_1 into roots of $G(y) = 0$, we are to prove that st transforms V_1 into some root. Suppose V_1 is transformed into V_s by s, into V_t by t, and into V_{st} by st. Then $G(V_1) = G(V_s) = G(V_t) = 0$, and we must show that $G(V_{st}) = 0$.

Now by Lemma 3 $V_s = \theta[V_1]$, a rational function (of V_1) with coefficients in R. Accordingly $G(\theta[V_1]) = 0$, which means that one root, V_1, of the Galois resolvent equation $G(y) = 0$ irreducible in R, satisfies $G(\theta[u]) = 0$. By Lemma 1 every root then of $G(y) = 0$ must satisfy $G(\theta[u]) = 0$, so that we have $G(\theta[V_t]) = 0$. Hence, $\theta(V_t)$ is one of the roots of $G(y) = 0$. But $\theta(V_t) = [\theta(V_1)]_t$; and since $\theta(V_1) = V_s$, then $[\theta(V_1)]_t = V_{st}$. That is, V_{st} is a root of $G(y) = 0$.

*Notes.** While $V_1 \equiv m_1x_1 + \cdots + m_nx_n$ may be chosen in many ways and the resulting Galois resolvents $G(y) = 0$ are many, still the group G of $f(x) = 0$ is always the same abstractly.

Using an $n!$-valued function is laborious when $n > 4$. Other methods have been devised.

67. Lagrange's and Galois' Theories. In proceeding to the Galois general equation we pause to contrast Lagrange's and Galois' viewpoints and to give some necessary definitions.

The idea of a number domain $R(k_1, \cdots, k_m)$ may be extended to a function-domain by saying that some or all of the k's shall be variables. We shall use $\Omega(k_1, \cdots, k_m)$ to indicate a domain of rationality whether it is a number or function domain.

If ϕ and ψ are polynomials in $x_1, \cdots, x_n$ with coefficients in

* *Cf.* Dickson, L. E., *Theory of Algebraic Equations* (1903), §§ 63, 65.

the domain $\Omega(k_1, \cdots, k_m)$, then $\phi = \psi$, (*i*) with Lagrange, if they are *formally* equal; (*ii*) with Galois if they are *numerically* equal for all numerical values that the x's and k's may assume. For example, if u and v are the roots of $x^2 + px + q = 0$, then (in the Galois sense) $q \cdot (u+v) = -puv$.

Again, in the Galois sense ϕ is invariant under a permutation s on $x_1, \cdots, x_n$, if s transforms ϕ into a polynomial *numerically* equal to ϕ.

Evidently, if functions are equal or invariant in the Lagrange sense, they are in the Galois sense, so that the theory preceding this section holds in the latter sense.

For the *general equation* $x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots + (-1)^n c_n = 0$ we consider the c's to be independent real or complex variables, and its *roots*, $x_1, \cdots, x_n$, to be n functions of the c's. For any set of values of the c's for which the discriminant of the equation does not vanish, there is a single set of distinct values for the roots.

68. Group of the General Equation. THEOREM C. *The group of a general nth degree algebraic equation in the domain R of its coefficients is the symmetric group of degree n.*

PROOF. The group of $x^n - c_1x^{n-1} + \cdots + (-1)^n c_n = 0$ will be shown to be the symmetric group of degree n if we can show that its Galois resolvent $G(y) = 0$ is of degree $n!$. Since $G(y) = 0$ is in domain R, its coefficients are expressible rationally in the c's. Expressing these c's in terms of the x's and remembering that $V_1 \equiv m_1x_1 + \cdots + m_nx_n$ is a $n!$-valued function, we have $G(V_1)$ as a polynomial in the x's. Hence, in $G(V_1)$ the coefficient of each x is zero, or $G(V_1) \equiv 0$.* Then under the symmetric group on $x_1, \cdots, x_n$, $G(V_1) = 0$ goes into $G(V_1) = 0$, $G(V_2) = 0$,

* *Cf.* Bôcher, M., *Higher Algebra* (1907), p. 5.

$G(V_3) = 0, \quad \cdots, \quad G(V_{n!}) = 0$. Since V_1 takes on $n!$ different values, $G(y) = 0$ is seen to have $n!$ distinct roots.

EXERCISES

1. Show that the domain $R(i)$ contains the rational domain. Is $x^2 + 1$ factorable in $R(i)$? Is $x^2 + 2$ factorable in $R(i)$?

$$(i = +\sqrt{-1}.)$$

2. If $i = +\sqrt{-1}$, determine whether $\sqrt{i}$ is an algebraic number. Determine whether $x^2 + 2 = 0$ is reducible in $R(\sqrt{2})$.

3. Prove: If $x^n + a_1x^{n-1} + \cdots + a_n = 0$ with coefficients in domain R has multiple roots, it is reducible in domain R.

4. Definition. A number is an **algebraic integer** if it satisfies an equation of the form $x^n + a_1x^{n-1} + \cdots + a_n = 0$ where the a's are rational integers. Determine whether $\dfrac{5 - \sqrt{-3}}{2}$ is an integer of the domain $R(\sqrt{-3})$.

5. Determine V_1 for the equation $x^3 - 2x^2 + x - 2 = 0$ in $R(1)$. Hint. Find the roots, then choose m's so that $V_1 \equiv m_1x_1 + m_2x_2 + m_3x_3$ has six different numerical values under the symmetric group of degree three.

6. Find for the equation $x^3 - 2x^2 + x - 2 = 0$, in $R(1)$, (*i*) a Galois resolvent $G(y) = 0$; (*ii*) its group.

7. If x_1, x_2, x_3, x_4 are the roots of $x^4 + 4 = 0$, has $V' = x_2 + 2x_3 + 3x_4$ 4! different numerical values under the symmetric group on x_1, x_2, x_3, x_4? Has $V'' = x_2 + 2x_3 + 4x_4$ 24 different values?

8. Work out a proof for Theorem *A* of § 66.

Hint. There are $n!(n! - 1)/2$ equations which these m's must not satisfy. Placing $m_1x_1 + \cdots + m_nx_n$ equal to its transform by (x_1x_2), gives $m_1 = m_2$, the only equation involving m_1 and m_2 alone. Select $m_1 \neq m_2$; then proceed to select m_3 so that no equation involving m_1, m_2, m_3 alone is satisfied. Etc.

69. Further Galois Theory. By adjunction Galois means obtaining a domain $\Omega'(h_1, \cdots, h_i, k_1, \cdots, k_m)$ from a domain $\Omega(k_1, \cdots, k_m)$ by introducing into the latter domain at least

one new quantity. Thus, $R(1, \sqrt{3})$ is obtained by adjoining $\sqrt{3}$ to $R(1)$. Note that $R(1, \sqrt{3}) \equiv R(\sqrt{3})$.

DEFINITION. If a group G on $x_1, \cdots, x_n$ has a subgroup H and the rational function $\phi(x_1, \cdots, x_n)$ is left unaltered numerically by permutations of H and by no others in G, then ϕ **is said to belong to the subgroup** H **of** G.

THEOREM D. *If H is a subgroup in a group G of an equation $f(x) = 0$ for a domain Ω, then there is a rational function with coefficients in Ω, of the roots which belongs to H.*

DEFINITION. If a rational function $\phi(x_1, \cdots, x_n)$ takes exactly ν values $\phi_1 \equiv \phi, \phi_2, \cdots, \phi_\nu$, when transformed by the symmetric group on $x_1, \cdots, x_n$, then $(y - \phi_1)(y - \phi_2) \cdots (y - \phi_\nu) = 0$ is called the **resolvent equation for** ϕ. (ν is $\leqslant n!$.)

THEOREM E. *If to the domain Ω of an equation $f(x) = 0$ is adjoined a rational function (with coefficients in Ω) of the roots, $\psi(x_1, \cdots, x_n)$, belonging to a subgroup H of the group G of $f(x) = 0$, the group of $f(x) = 0$ is reduced to H; and if H is of index ν in G, the permutations of G transform ψ into exactly ν numerically distinct functions which are the roots of the resolvent equation $G(y) \equiv (y - \psi_1)(y - \psi_2) \cdots (y - \psi_\nu) = 0$ which is in Ω, is irreducible in Ω and has G/H for its group.*

THEOREM F. *If p is a prime, the binomial equation $x^p = A$ can be solved by (or is equivalent to) a chain of equations the group of each being a regular cyclic group of prime order for a certain domain.*

THEOREM G. GALOIS THEOREM. *By adjoining any root of the equation $F(x) = 0$, whose group in R is a regular cyclic group of prime order p, to R in which is the equation of $f(x) = 0$,*

the group of $f(x) = 0$ either is not reduced or is reduced to an invariant subgroup of index p.

70. **Criterion of Solvability.** The algebraic equation $x^n - c_1x^{n-1} + c_2x^{n-2} - \cdots + (-1)^n c_n = 0$ is **solvable by radicals** with respect to the domain $\Omega(k_1, \cdots, k_m)$ containing its coefficients, if its roots can be obtained from $k_1, \cdots, k_m$ by addition, subtraction, multiplication, division, and the extraction of a root of any index,* these operations being finite in number.

THEOREM H. *If the group G of an equation $f(x) = 0$ is of prime order p for a domain $\Omega(k_1, \cdots, k_m)$, then the equation is solvable by radicals in Ω; i.e., the roots are rational functions of the k's and an imaginary pth root of unity.*

Proof of the preceding theorem will be omitted, but we shall use the theorem in sketching a proof of the generalized Galois Criterion.

THEOREM I. CRITERION. *A necessary and sufficient condition that an algebraic equation be solvable by radicals in a domain Ω containing its coefficients is that all the composition-factors of its group for Ω be prime integers.*

SUFFICIENCY. Induction will be employed in the proof here. By the preceding theorem the Galois Criterion is seen to hold when there is but one composition-factor and it is prime. Assume the criterion true when the composition-factors of the group G of the given equation consist of $\lambda(\lambda > 1)$ primes. Now G must contain an invariant subgroup H whose index is some one of the primes, say p, of the series of composition-factors (§ 53). By Theorem D there exists a rational function ψ in $\Omega(k_1, \cdots, k_m)$ of the roots, which belongs to H. This we adjoin

* But not necessarily the extraction of *all* roots of that index.

to Ω giving $\Omega'(\psi, k_1, \cdots, k_m)$ and a resolvent equation in $\Omega(k_1, \cdots, k_m)$,

$$G(y) \equiv (y-\psi_1)(y-\psi_2)\cdots(y-\psi_p) = 0, \text{ where } \psi_1 \equiv \psi,$$

and reducing the group of $f(x) = 0$ from G with respect to Ω to H with respect to Ω'. (By Theorem E.) From the preceding Theorem, $G(y) = 0$ is solvable rationally in $k_1, \cdots, k_m$, and an imaginary pth root of unity. Substituting in Ω' the value of ψ_1 thus found and remembering that the criterion is here assumed to hold for $< \lambda$ prime composition-factors and that H has exactly $\lambda - 1$ prime composition-factors, we have a proof for the case of λ prime composition-factors.

The inductive method just used somewhat obscures the fact that there is a chain of resolvent equations $G_1(y_1) = 0, G_2(y_2) = 0$, etc., and that corresponding to each there is a group for its particular domain, G/H_1, H_1/H_2, etc., the orders of the groups being respectively primes, p_1, p_2, etc.

Necessity. We assume here that $f(x) = 0$ is solvable by radicals in a domain Ω containing its coefficients, and we must show that the composition-factors of the group G of $f(x) = 0$ for Ω are prime integers. Now every root is by assumption deducible by rational operations and root extractions of quantities from the domain $\Omega(k_1, \cdots, k_m)$ or of quantities obtained from these by such operations. Since $u^{pq} = c$ may be replaced by $u^p = v$ and $v^q = c$, we may take the index of each radical in every root of $f(x) = 0$ to be a prime. Any such radical would be a root of a binomial equation, which by Theorem F would be equivalent to a chain of equations each with a regular cyclic group of prime order. Now adjoin to Ω a root r_1 of the first equation of the chain, then a root r_2 of the second equation of the chain, etc., giving $\Omega'(r_1, \cdots, k_1, \cdots, k_m)$. On continuing

adjoining roots from the equations of any other chains, we would ultimately enlarge Ω to contain all the roots of $f(x) = 0$, and thus with respect to this enlarged domain the group of $f(x) = 0$ would be the identity (by Theorem B).

But by Theorem G, in each adjunction the group in question either is not reduced or else is reduced to an invariant subgroup of prime index. The series of groups from G to the identity thus forms a composition-series with prime composition-factors.

As a sort of corollary we have the following

THEOREM J. *The general nth degree algebraic equation is solvable by radicals in the domain of its coefficients if and only if* $n < 5$.

For, from § 68 the group of the general nth degree equation is the symmetric group on n letters, which is solvable if and only if $n < 5$ (by p. 123, Ex. 2).

71. Examples of Adjunction. EXAMPLE 1. For $R(1)$ the group of $x^3 - 2x^2 + x - 2 = 0$ is of order and degree 2. (*Cf.* p. 147, Ex. 6.) If to $R(1)$ is adjoined one of the roots not in $R(1)$, as i, we have $R(1, i)$. Any Galois resolvent of $x^3 - 2x^2 + x - 2 = 0$ for $R(1, i)$ is a linear equation. This means that the roots of the given equation are numbers in $R(1, i)$, which is obvious since they are $2, +i, -i$. $(i = +\sqrt{-1}.)$

EXAMPLE 2. It is not difficult to show that for the roots of $f(x) \equiv x^4 - 4x^2 + 1 = 0$, $V_1 \equiv x_1 + 2x_2 + 5x_3$ is a 4!-valued function under the symmetric group on x_1, x_2, x_3, x_4. If the roots are $x_1 = -x_3 = \sqrt{2 + \sqrt{3}}$, $x_2 = -x_4 = \sqrt{2 - \sqrt{3}}$, one Galois resolvent equation in $R(1)$ is

$$[y - (x_1 + 2x_2 + 5x_3)][y - (5x_1 + x_3 + 2x_4)] \cdot$$
$$[y - (2x_1 + x_2 + 5x_4)][y - (5x_2 + 2x_3 + x_4)]$$

$$\equiv [y^2 - 12(2+\sqrt{3})]\cdot[y^2 - 12(2-\sqrt{3})]$$
$$\equiv y^4 - 48\,y^2 + 144 = 0.$$

Hence the group of $f(x) = 0$ is

$$G \equiv [I,\ (x_1x_3)(x_2x_4),\ (x_1x_2)(x_3x_4),\ (x_1x_4)(x_2x_3)] \text{ for } R(1),$$

because these permutations are the only ones of the symmetric group on x_1, x_2, x_3, x_4 transforming V_1 into the V's of the Galois resolvent. (Theorem B.) Now $x_1 + x_2 \equiv \sqrt{2+\sqrt{3}} + \sqrt{2-\sqrt{3}}$ belongs to the subgroup $H \equiv [I,\ (x_1x_2)(x_3x_4)]$ of G (by definition in § 69); hence, by Theorem E H is the group of $f(x) = 0$ for the enlarged domain $R(1, \sqrt{2+\sqrt{3}} + \sqrt{2-\sqrt{3}})$. Continuing, we see that the function $x_1 \equiv \sqrt{2+\sqrt{3}}$ belongs to the identity in H; hence, the identity is the group of $f(x) = 0$ for the domain $R(1,\ \sqrt{2+\sqrt{3}} + \sqrt{2-\sqrt{3}},\ \sqrt{2+\sqrt{3}})$. By noting that $R(1,\ \sqrt{2+\sqrt{3}} + \sqrt{2-\sqrt{3}},\ \sqrt{2+\sqrt{3}}) \equiv R(1,\ \sqrt{2+\sqrt{3}},\ \sqrt{2-\sqrt{3}}) \equiv R(\sqrt{2+\sqrt{3}})$, we see that the roots of $f(x) = 0$ are in the domain finally reached.

Example 3. The roots of $x^3 - 16 = 0$ are

$$x_1 = 2\sqrt[3]{2},\ x_2 = (-1 + \sqrt{3}\,i)\sqrt[3]{2},\ x_3 = (-1 - \sqrt{3}\,i)\sqrt[3]{2}.$$

Now under the symmetric group on x_1, x_2, x_3, the function $x_1 + 2x_2$ is 3!-valued, and for domain $R(1)$ the Galois resolvent equation here is

$$[y - (x_1 + 2x_2)][y - (x_1 + 2x_3)][y - (2x_2 + x_3)]\cdot$$
$$[y - (2x_1 + x_3)][y - (x_2 + 2x_3)][y - (2x_1 + x_2)]$$
$$\equiv [y^3 + 12\sqrt[3]{4}][y^2 - 6(1 - 3\,i)\sqrt[3]{4}][y^2 - 6(1 + 3\,i)\sqrt[3]{4}]$$
$$\equiv y^6 - 6912 = 0.$$

Then by Theorem B, the group of $x^3 - 16 = 0$ for $R(1)$ is

$$G \equiv [I,\ (x_1x_2),\ (x_1x_3,)\ (x_2x_3),\ (x_1x_2x_3),\ (x_1x_3x_2)].$$

The function $\dfrac{x_2 - x_3}{x_1} = \sqrt{3}\,i$ is seen to belong to the subgroup $H \equiv [I, (x_1x_2x_3), (x_1x_3x_2)]$ of G (by definition in § 69); hence, by Theorem E H is the group of $x^3 - 16 = 0$ for $R(1, \sqrt{3}\,i) \equiv R(\sqrt{3}\,i)$. Finally, we see that $x_1 = 2\sqrt[3]{2}$ belongs to the identity in H. Hence I is the group of $x^3 - 16 = 0$ for $R(\sqrt{3}\,i, \sqrt[3]{2})$, in which domain are the roots of the given equation.

EXERCISES

1. If x_1, x_2, x_3 are the roots of $x^3 + x^2 + 1 = 0$, show that in the Lagrange sense $x_2(x_1x_2 + x_2x_3) = 1$ belongs to $[I, (x_1x_3)]$, while in the Galois sense it belongs to the symmetric group on x_1, x_2, x_3.

2. Apply Galois' Criterion to each of the following equations to determine whether or not it is solvable in the domain indicated (see §§ 53, 55).

(*a*) $x^4 + 1 = 0$ whose group for $R(1)$ is the four-group.

(*b*) $x^3 - 3x - 1 = 0$ whose group for $R(1)$ is the cyclic group of order 3.

(*c*) $x^3 - 5 = 0$ whose group for $R(1)$ is the symmetric group of degree 3.

(*d*) $x^3 - 3x - \sqrt{2} = 0$ whose group for $R(\sqrt{2})$ is of order 2.

(*e*) A certain quartic equation whose group is the octic group of degree 4.

(*f*) $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$ (p an odd prime) whose group for $R(1)$ is a regular cyclic group of order $p - 1$.

(*g*) $x^5 + a_1x^4 + \cdots + a_5 = 0$ whose group for $R(1)$ is the symmetric group of degree 5. (The a's are assumed rational.)

3. Find the group of $(x - \sqrt{2})(x + 2)(x + \sqrt{2}) = 0$ for $R(1)$.

4. Find the group of $x^3 - 3x - 1 = 0$ in $R(1)$ without using a V. Suggestion. G is the symmetric group of degree 3 or is one of its subgroups. How can I be excluded? G is not the symmetric group itself nor a subgroup of order 2, for by using

$$\psi \equiv (x_1 - x_2) \cdot (x_2 - x_3) \cdot (x_3 - x_1),$$

which is the square-root of the discriminant and here equals ± 9,

and adjoining 9 to $R(1)$, the domain of the coefficients, there results a contradiction or an impossibility (by Theorem E).

5. Make a study of $x^4 + 4 = 0$ similar to the discussion in Example 2 of § 71. Hint. See p. 147, Ex. 7.

6. Make a study of $x^3 + 40 = 0$ similar to the discussion in Example 3 of § 71.

7. Find the group of $x^4 + 16 = 0$ for the domain $R(i)$.

8. It can be proved that for a domain R the group of $f(x) \equiv x^n + a_1x^{n-1} + \cdots + a_n = 0$ is transitive on $x_1, x_2, \cdots, x_n$ if $f(x)$ is irreducible in R, intransitive if $f(x)$ is reducible in R. Verify this proposition in the Examples of § 71 and in Exercises 2–7 in this set.

CONSTRUCTIONS BY RULER AND COMPASSES

72. On Constructibility. In plane geometry we learned how to perform addition, subtraction, multiplication, division, and square-root for given line segments (including when necessary a segment of unit length), by ruler and compasses. The geometric construction of $\frac{1}{2}\sqrt{a - \sqrt{bc}}$ involves merely a succession of such operations.

Conversely, if a plane construction is possible by ruler and compasses, it is seen from analytical geometry to involve only equations of the first and second degrees. The simultaneous solution of such equations is known to require but rational operations and square roots. (The given elements must be real.)

Hence, *a construction is possible by ruler and compasses when and only when the required magnitude can be expressed in terms of the given (real) magnitudes by means of a finite number of rational operations and real square roots.* (Compare with "*solvable* by radicals" (§ 70) in which extraction of a root of any index is admitted.)

Since adjoining a (constructible) square root to a domain of

an algebraic equation would at most reduce the group of the equation to an invariant subgroup of index 2 (Galois' Theorem, § 69), *the roots of an algebraic equation are not constructible by ruler and compasses if any composition-factor of its group is different from* 2.

We shall now apply this proposition to treat two of the famous problems first studied by the early Greek mathematicians.

Duplication of the Cube.* Using the edge of the given cube as unity, the edge of the required cube of double the volume is a real root of $z^3 = 2$. The group of this equation for $R(1)$ is the symmetric group of order 6, as is easily seen by putting $x = 2z$ in Example 3 of § 71. Hence, it is impossible to construct with ruler and compasses the side of a cube whose volume is double that of a given cube.

Trisection of an Angle. To prove that not every given angle can be trisected with ruler and compasses, we shall show that the angle 60° cannot be thus trisected. If 60° could be trisected, cos 20° could be constructed with ruler and compass (with only a line of unit length given); and conversely.

From trigonometry $4\cos^3\theta - 3\cos\theta = \cos 3\theta$.
Putting $x = 2\cos\theta$ gives $x^3 - 3x = 2\cos 3\theta$.
Now x is constructible if and only if $\cos\theta$ is constructible.
Putting $\theta = 20°$, we have

$$x^3 - 3x - 1 = 0.$$

By p. 153, Exercise 4, the group of this equation for $R(1)$ is a cyclic group of order 3. Hence x, cos 20°, and 20° are not constructible with ruler and compasses.

* The "Delian Problem." See W. W. R. Ball's *Mathematical Recreations and Essays* or histories of mathematics.

COROLLARY. *It is impossible to construct with ruler and compasses a regular polygon with* $2^n 9$ *sides.* ($n = 0, 1, 2,$ *etc.*)

EXERCISES

1. If the coefficients and one root of a given cubic equation are constructible with ruler and compasses, show that the two other roots are constructible if real. Hint. Depress the cubic equation.

State a similar proposition for a quartic equation.

2. In what domain are the roots of $x^3 - 3x - \sqrt{2} = 0$ if one root is $-\sqrt{2}$? What can you infer is the group of $x^3 - 3x - \sqrt{2} = 0$ for the domain $R(\sqrt{2})$? For the domain $R(\sqrt{2}, \sqrt{3})$?

3. Verify by the theory here that an angle of 45° can be trisected. Hint. Put $\theta = 15°$ in the equation $x^3 - 3x - 2\cos 3\theta = 0$ of this section and use the preceding exercise.

A NOTE ON LIE'S THEORY

73. A One-parameter Transformation Group. We here give a suggestion of Lie's application of one-parameter groups to ordinary differential equations. The student is referred to introductory textbooks for more information.*

A one-parameter transformation in two variables x, y and parameter t may be written as follows:

$$x_1 = \phi(x, y, t),$$
$$y_1 = \psi(x, y, t).$$

EXAMPLE 1. $x_1 = x + t$, $y_1 = y$.

An infinitesimal transformation is of the form

$$x_1 = \phi(x, y, t_0 + \delta t),$$
$$y_1 = \psi(x, y, t_0 + \delta t),$$

* Page, J. M., *Ordinary Differential Equations* (1897); Campbell, J. E., *Theory of Continuous Groups* (1903); Cohen, A., *The Lie Theory of One-parameter Groups* (1911).

which by Taylor's expansion gives

$$\delta x = \left(\frac{\partial \phi}{\partial t}\right)_{t_0} \delta t + \cdots, \quad \delta y = \left(\frac{\partial \psi}{\partial t}\right)_{t_0} \delta t + \cdots.$$

Neglecting higher powers of δt and using $\zeta(x, y) \equiv \left(\frac{\partial \phi}{\partial t}\right)_{t_0}$,

$$\eta(x, y) \equiv \left(\frac{\partial \psi}{\partial t}\right)_{t_0},$$

we have

$$\begin{aligned} \delta x &= \zeta(x, y)\delta t, \\ \delta y &= \eta(x, y)\delta t. \end{aligned} \tag{2}$$

EXAMPLE 2. For Example 1, $\delta x = \delta t$, $\delta y = 0$, $\zeta = 1$, $\eta = 0$.

Lie employed Uf to indicate the effect of the infinitesimal transformation (2) on the function $f(x, y)$, so that

$$Uf \equiv \zeta \frac{\partial f}{\partial x} + \eta \frac{\partial f}{\partial y}, \text{ or } \equiv \left(\frac{\partial \phi}{\partial t}\right)_{t_0} \frac{\partial f}{\partial x} + \left(\frac{\partial \psi}{\partial t}\right)_{t_0} \frac{\partial f}{\partial y}.$$

Equations (2) can be shown to give rise to

$$\begin{aligned} u(x_1, y_1) &= u(x, y), \\ v(x_1, y_1) &= v(x, y) + t. \end{aligned} \tag{3}$$

The transformations resulting from giving t all values in (3) constitute a group of one parameter called the group generated by the infinitesimal transformation (2).

74. Some Theorems. THEOREM 1. *If and only if* $Uf = 0$, *is the function* $f(x, y)$ *invariant (formally) under the group* Uf.

EXAMPLE 3. If $f(x, y)$ is $\frac{x^2 + y^2}{x^2}$ and $x_1 = tx$, $y_1 = ty$; then

$\zeta = (x)_{t=0} = x$, $\eta = (y)_{t=0} = y$.

Uf is $x \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y}$, which is $x\left(\frac{-2y^2}{x^3}\right) + y\left(\frac{2y}{x^2}\right)$. Since this

vanishes, $\frac{x^2+y^2}{x^2}$ is invariant under the given transformation. Verify this.

THEOREM 2. *If and only if $Uf = a$ function of f, is the family of curves $f(x, y) = c$ invariant under the transformation Uf.*

THEOREM 3. *If and only if* $\zeta\frac{\partial f}{\partial x}+\eta\frac{\partial f}{\partial y}+\left(\frac{d\eta}{dx}-y'\frac{d\zeta}{dx}\right)\frac{\partial f}{\partial y'}=0$ *when $f(x, y, y') = 0$, is the differential equation $f(x, y, y') = 0$ invariant under the transformation* $Uf=\zeta\frac{\partial f}{\partial x}+\eta\frac{\partial f}{\partial y}$.

From the study of elementary differential equations we know that $P(x, y)\,dx+Q(x, y)\,dy = 0$, a linear differential equation of the first order, is *exact* if and only if $\frac{\partial P}{\partial y}=\frac{\partial Q}{\partial x}$.

LIE'S THEOREM.* *If the family of integral curves of the differential equation $M(x, y)dx+N(x, y)dy = 0$ is invariant under the group* $Uf\equiv\zeta\frac{\partial f}{\partial x}+\eta\frac{\partial f}{\partial y}$ *and if* $\zeta M+\eta N\not\equiv 0$, then $\frac{Mdx+Ndy}{\zeta M+\eta N}=0$ *is exact.*†

PROOF. According to the observation made just before the Theorem we must show that

$$\frac{\partial}{\partial y}\left\{\frac{M}{\zeta M+\eta N}\right\}=\frac{\partial}{\partial x}\left\{\frac{N}{\zeta M+\eta N}\right\}.$$

* Lie, S., *Verhandlungen der Gesellschaft der Wissenschaften zu Christiania*, November, 1874.

† In other words, $\frac{1}{\zeta M+\eta N}$ is Euler's *integrating factor*.

If $f(x, y) = c$ is the family of integral curves of $M dx + N dy = 0$ then $\frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = 0$, so that $\frac{\partial f}{\partial x} / M = \frac{\partial f}{\partial y} / N$.

From the hypothesis, $f(x, y) = c$ is invariant under Uf, so that by Theorem 2 $\xi \frac{\partial f}{\partial x} + \eta \frac{\partial f}{\partial y} = F(f)$.

Then $$\frac{M}{\xi M + \eta N} = \frac{\frac{\partial f}{\partial x}}{\xi \frac{\partial f}{\partial x} + \eta \frac{\partial f}{\partial y}} = \frac{\frac{\partial f}{\partial x}}{F(f)};$$

and $$\frac{N}{\xi M + \eta N} = \frac{\frac{\partial f}{\partial y}}{\xi \frac{\partial f}{\partial x} + \eta \frac{\partial f}{\partial y}} = \frac{\frac{\partial f}{\partial y}}{F(f)}.$$

It is now easy to show that $\frac{\partial}{\partial y}\left\{\frac{\frac{\partial f}{\partial x}}{F(f)}\right\} = \frac{\partial}{\partial x}\left\{\frac{\frac{\partial f}{\partial y}}{F(f)}\right\}$,

thereby establishing the theorem.

75. An Application. In applying the theory, the converse of the theorem just demonstrated is more direct. It consists in finding the general type of differential equation whose integral curves are invariant under a given group. We illustrate this by the following

EXAMPLE 4. Find all first-order differential equations whose integral curves are invariant under the transformation $Uf \equiv x \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y}$. (Note. From Ex. 3, p. 157 we see that geo-

metrically this is the *perspective transformation*, $x_1 = tx$, $y_1 = ty$.)

Here $\zeta = x$ and $\eta = y$, so that $\frac{d\eta}{dx} - y'\frac{d\zeta}{dx}$ of Theorem 3 gives $\frac{dy}{dx} - y', = 0$. Hence, $\zeta\frac{\partial f}{\partial x} + \eta\frac{\partial f}{\partial y} + \left(\frac{d\eta}{dx} - y'\frac{d\zeta}{dx}\right)\frac{\partial f}{\partial y'} = 0$ is $x\frac{\partial f}{\partial x} + y\frac{\partial f}{\partial y} + 0 \cdot \frac{\partial f}{\partial y'} = 0$. Thence, by the theory of partial differential equations we have the following Lagrangean equations:

$$\frac{dx}{x} = \frac{dy}{y} = \frac{dy'}{0}.$$

Solving, we obtain $f(y', y/x) = 0$, or $y' = F\left(\frac{y}{x}\right)$, an equation which is homogeneous in x and y.

COROLLARY. *In $Mdx + Ndy = 0$ if M and N are homogeneous in x and y and of the same degree, $\frac{Mdx + Ndy}{Mx + Ny} = 0$ is exact.* ($Mx + Ny \not\equiv 0$.)

This follows from Example 4 because of Lie's Theorem.

EXERCISES

1. Complete the proof of Lie's Theorem by showing that

$$\frac{\partial}{\partial y}\left\{\frac{\frac{\partial f}{\partial x}}{F(f)}\right\} = \frac{\partial}{\partial x}\left\{\frac{\frac{\partial f}{\partial y}}{F(f)}\right\}$$

2. Show that for an infinitesimal rotation the transformation $x_1 = x\cos\theta - y\sin\theta$, $y_1 = x\sin\theta + y\cos\theta$, gives $\zeta = -y$, $\eta = x$. Then find the function $f(x, y)$ which is invariant under the group $Uf \equiv -y\frac{\partial f}{\partial x} + x\frac{\partial f}{\partial y}$. (See Theorem 1 of p. 157.)

3. Find all first-order differential equations whose integral curves are invariant under the *affine transformation* group, $Uf = x\dfrac{\partial f}{\partial x}$.

4. It can be shown that $y' + P(x)y = Q(x)$, the general linear differential equation of the first order, is invariant under the group $Uf \equiv e^{-\int P dx}\cdot\dfrac{\partial f}{\partial y}$. (P. 161, Ex. 6.) Assume this and employ Lie's Theorem to find an integrating factor for the differential equation and show that its use does make the equation exact.

ADDITIONAL EXERCISES

1. Prove the fundamental theorem of symmetric functions. *Cf.* Cajori's *Theory of Equations* (1904), § 70, or other books on the theory of equations.

2. If p is a prime, $x^{p-1} + x^{p-2} + \cdots + x + 1 = 0$ is called a cyclotomic equation. Prove that a cyclotomic equation is irreducible in the rational realm. *Cf.* Dickson, L. E., *Modern Algebraic Theories* (1926), § 83.

3. For a proof of the theorem in Exercise 8 of p. 154, see Dickson, L. E., *Theory of Algebraic Equations* (1903), § 68; or his *Modern Algebraic Theories* (1926), § 90.

4. For discussions of constructions by ruler and compasses including the construction of a regular n-sided polygon, see Cajori's *Theory of Equations* (1904), § 183 and its exercises; or Miller, Blichfeldt, and Dickson, *Finite Groups* (1916), Chapter XVII, etc.

5. Find all first-order differential equations whose integral curves are invariant under rotation (*cf.* Ex. 2 of p. 160), and by use of Lie's Theorem determine an integrating factor for the equations. *Cf.* Page, J. M., *Ordinary Differential Equations* (1897), § 66; or Cohen, A., *Lie Theory of One-parameter Groups* (1911), p. 53.

6. Find all first-order differential equations that are invariant under the group $Uf \equiv e^{-\int P(x)dx}\dfrac{\partial f}{\partial y}$. *Cf.* Ex. 4 of p. 161. Suggestion. Work like Example 4 of § 75. See Page, *Ordinary Differential Equations* (1897), § 68; or, Cohen, *Lie Theory of One-parameter Groups* (1911), p. 56.

INDEX

Abbati, 24
Abel, 26
Abelian groups, 26, 87–94, 96, 110, 112, 113
Absolute invariant, 132
Abstract definitions of groups, 95–106
Adjunction, 147, 151
Affine transformation, 161
Algebraic integer, 147
Algebraic number, 142
Alternating group, 28
Automorphism, 107

Bilinear form, 129
Bolza, 52
Burnside, 137

Carmichael, 24
Cauchy, theorem, 83
Cayley's color groups, 73
  multiplication table, 22
  notation, 58, 61
  theorem, 28
Central, 26
Characteristic
  element, subgroup, 107
  equation, 133
  of a substitution, 140
Characteristic series, 123
Chief-series, 122
Circular permutation, 11
Class, 36
Closed set, 2
Cogredient isomorphism, 109
Color groups, 73
Commutative, 3, 19
Commutator, 19
Commutator subgroup, 78
Complete group, 109
Completely reducible group, 138
Complete residue system, 70
Composite group, 55
Composition-factors, 119
Composition-factor-groups, 118
Composition-series, 118
Congruence groups, 69
Conjugate-imaginary groups, 128
Conjugate of linear substitution, 127
Conjugate set of elements, 37
  of subgroups, 39
Construction of intransitive groups, 52
Constructions by ruler and compasses, 154
Contragredient isomorphism, 109
Co-sets, 25
Criterion of solvability, 149
Cross-cut, 41
Cross-ratio group, 73
Cycle, 11
Cyclic group, 6
Cyclotomic equation, 161

Dedekind, 104
Degree, 10
Delian Problem, 155
Derived groups, series of, 123
Dickson, 141
Dicyclic group, 96
Dihedral groups, 64, 96
Direct products, 52
Domain, 142
  equation in, 142
  function in, 142
Doubly transitive, 43
Duplication of cube, 155
Dyck, theorem, 76

Element, 3
Elementary symmetric functions, 141
Euler-Fermat theorem, 88, 118
Euler's integrating factor, 158
Even permutation, 19

Fermat's minor theorem, 88, 118
Four-group, 33, 72
Frobenius, theorems, 35, 86, 124, 139
Function-domain, 145

Galois, 24
  criterion, 149
  function, 143
  resolvent, 143
  theory, 141–153
General isomorphism, 51
Generators, 15, 87, 92
  independent, 95
Group, defined, 6
Group of an equation, 145
Group of automorphisms, 108
Group of isomorphisms, 107–117
Group of one parameter, 156
Group property, 2
Groups of movements, 1, 3, 62–67

Hamiltonian groups, 104
Head, 80
Hermite, 142
Hermitian form, 129
  positive-definite form, 129
Hermitian substitution, 127
Hölder, theorem, 120
Holomorph of a regular group, 110

Identity, 3, 6, 10, 126
Imprimitive group, 45
Index of a subgroup, 25
Infinite group, 7, 65
Inner isomorphism, 109, 110
Insolvable group, 121
Intransitive group, 33
Invariant, absolute, 132
  element, 19
  relative, 132
  set, 20
  subgroup, 20
Invariants of abelian group, 92
Inverse, 3, 16, 126
Irreducible equation, function, 142
Irreducible group, 136
Isomorphism method, 52
Isomorphisms, 49
Isomorphisms, group of, 107–117

Jordan, theorems, 32, 120, 121

k-ply transitive, 43
Kronecker, theorem, 93

Lagrange, theorem, 24
Lagrange's and Galois' theories, 145
Latin square, 22
Lie's theory, 156–160
  theorem, 158
Lindemann, 142
Linear fractional substitution, 128
Linear substitution, 125
Linear substitution group, 127
Loewy, theorem, 132

Manning, 137
Mathewson, 81, 91, 118
Matrices as group elements, 71
Maximum invariant subgroup, 76
Maximum subgroup, 76
Metabelian group, 80
Metacyclic group, 121
Miller, theorems, 27, 41, 43, 61, 106, 113, 114, 115, 116, 118
Multiple transitivity, 43
Multiplication table of group, 22

Negative permutation, 19
Netto, theorum, 20
Non-abelian group, 26

Non-commutative, 3, 5
Non-singular linear substitution, 125
Non-twelve group, 106
Number domain, 142
Number theory notes, 88

Octahedron, group of, 73
Octic group, 34
Odd permutation, 19
One-parameter transformation group, 156
Operator, 3
Order, 3
Orthogonal substitution, 140
Outer isomorphism, 109, 110

Perfect group, 78
Period, 6
Permutation, 10
Permutation groups, 8–61
Perspective transformation, 160
Positive permutation, 19
Prime-power, abelian groups, 91
  groups, 98
  subgroups, 82
Primitive group, 45
Primitive root, 88

Quaternion group, 71
Quaternion units as elements, 71
Quotient group, 54

Radicals, solvable by, 149
Ranum, 112
Rational operations, 141
Realm, number, 142
Reduced residue system, 70
Reducible equation, 142
Reducible group, 136
Reducible in a domain, 142
Regular permutation, 12
Regular permutation group, 12
Relative invariant, 132
Resolvent equation, 148

Self-conjugate subgroup, 20
Semi-group, 7
Similar permutations, 12
Simple group, 55
Simple isomorphism, 50
Simply transitive, 43
Solvable by radicals, 149
Solvable group, 121
Subgroup, 17
Substitution, 10
  conjugate, 127
  Hermitian, 127
  identical, 126
  inverse, 126
  linear, 125
  linear fractional, 128
  symmetric, 127
Sylow, theorems, 83, 98
Sylow subgroup, 83
Symmetric function, 17, 22, 141
  fundamental theorem of, 161
Symmetric group, 15, 16
Symmetric Hermitian substitution, 127
Systems of imprimitivity, 45

Tetrahedron, group of, 64
Transcendental number, 142
Transform, 19
Transitive group, 33 *et seq.*
Transposition, 10
Triply transitive, 43
Trisection of an angle, 155
Type of an abelian group, 92

Vandermonde, determinant of, 19

Weisner, theorem of, 86
Wilson's theorem, 88, 116
Winger, 73

Young, theorem, 124

Date Due

DE 24			
JA 6 '48			
MY 14'48			
FE 23'50			
SEP 18 1957			
DEPARTMENT			
FEB 2 1963			
MY 21'68			

CONNECTICUT COLLEGE LIBRARY
512.86 M426
Elementary theory of finite groups.
dc
3 1839 001960792

512.86
M426

93397

Mathewson

Elementary theory of finite groups

DATE DUE	BORROWER'S NAME

512.86
M426

93397